LINKSYS®
A Division of Cisco Systems, Inc.

2,4 GHz 802.11g

# Wireless-G

WIRELESS

## ADSL-Gateway mit SRX200

# Benutzerhandbuch

Modell-Nr. **WAG54GX2 (DE) Annex B**

CISCO SYSTEMS

## Copyright und Marken

Technische Änderungen vorbehalten. Linksys ist eine eingetragene Marke bzw. eine Marke von Cisco Systems, Inc. und/oder deren Zweigunternehmen in den USA und anderen Ländern. Copyright © 2005 Cisco Systems, Inc. Alle Rechte vorbehalten. Andere Handelsmarken und Produktnamen sind Marken bzw. eingetragene Marken der jeweiligen Inhaber.

## Hinweise zur Verwendung dieses Handbuchs

Ziel des Benutzerhandbuchs zum Wireless-G ADSL-Gateway mit SRX200 ist, Ihnen den Einstieg in den Netzwerkbetrieb mit dem Gateway noch weiter zu erleichtern. Achten Sie beim Lesen dieses Benutzerhandbuchs auf Folgendes:

Dieses Häkchen kennzeichnet einen Hinweis, den Sie bei Verwendung des Gateways besonders beachten sollten.

Dieses Ausrufezeichen kennzeichnet eine Warnung und weist darauf hin, dass unter bestimmten Umständen Schäden an Ihrem Eigentum oder am Gateway verursacht werden können.

Dieses Fragezeichen dient als Erinnerung an bestimmte Schritte, die bei Verwendung des Gateways durchzuführen sind.

Neben den Symbolen finden Sie Definitionen für technische Begriffe, die in folgender Form dargestellt werden:

***Wort:*** *Definition.*

Alle Abbildungen (Diagramme, Bildschirmdarstellungen und andere Bilder) sind mit einer Abbildungsnummer und einer Kurzbeschreibung versehen (siehe folgendes Beispiel):

**Abbildung 0-1: Kurzbeschreibung der Abbildung**

Die Abbildungsnummern und die zugehörigen Kurzbeschreibungen finden Sie auch im Inhalt unter „Abbildungsverzeichnis“.

# Inhalt


Kapitel 1: Einführung 1
- Willkommen 1
- Inhalt dieses Benutzerhandbuchs 2

Kapitel 2: Planen des Netzwerks 4
- Funktionen des Gateways 4
- IP-Adressen 4

Kapitel 3: Beschreibung des Wireless-G ADSL-Gateways mit SRX200 6
- Ports und Taste „Reset“ an der Geräteseite 6
- LEDs an der Geräteseite 7

Kapitel 4: Anschließen des Wireless-G ADSL-Gateways mit SRX200 8
- Übersicht 8
- Verdrahtete Verbindung mit einem Computer 9
- Wireless-Verbindung mit einem Computer 10

Kapitel 5: Einrichten des Wireless-G ADSL-Gateways mit SRX200 12
- Übersicht 12
- Verwenden des Setup-Assistenten 12

Kapitel 6: Konfigurieren des Wireless-G ADSL-Gateways mit SRX200 26
- Übersicht 26
- Hinweis für den Zugriff auf das webbasierte Dienstprogramm 29
- Registerkarte „Setup“ (Einrichtung) 29
- Registerkarte „Wireless“ 38
- Registerkarte „Security“ (Sicherheit) 45
- Registerkarte „Access Restrictions“ (Zugriffsbeschränkungen) 53
- Registerkarte „Applications & Gaming“ (Anwendungen und Spiele) 55
- Registerkarte „Administration“ (Verwaltungsfunktionen) 62
- Registerkarte „Status“ 67

Anhang A: Fehlerbehebung 71
- Behebung häufig auftretender Probleme 71
- Häufig gestellte Fragen 81

Anhang B: Wireless-Sicherheit 89
- Vorsichtsmaßnahmen 89
- Sicherheitsrisiken bei Wireless-Netzwerken 89

Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters 92
Anweisungen für Windows 98/ME 92
Anweisungen für Windows 2000/XP 93
Anhang D: Aktualisieren der Firmware 94
Anhang E: Glossar 95
Anhang F: Spezifikationen 102
Anhang G: Garantieinformationen 104
Anhang H: Zulassungsinformationen 106
Anhang I: Kontaktinformationen 113

# Abbildungsverzeichnis

Abbildung 2-1: Netzwerk 4
Abbildung 3-1: Ports und Taste „Reset“ an der Geräteseite 6
Abbildung 3-2: LEDs an der Geräteseite 7
Abbildung 4-1: Herstellen der ADSL-Verbindung 9
Abbildung 4-2: Anschließen eines PCs 9
Abbildung 4-3: Anschließen des Netzstroms 9
Abbildung 4-4: Herstellen der ADSL-Verbindung 10
Abbildung 4-5: Anschließen des Netzstroms 11
Abbildung 5-1: Setup-Assistent – Willkommensfenster – Sprachauswahl 12
Abbildung 5-2: Setup-Assistent – Willkommensfenster – Fenster zum Starten des Assistenten 12
Abbildung 5-3: Setup-Assistent – Fenster License Agreement (Lizenzvereinbarung) 13
Abbildung 5-4: Setup-Assistent – Fenster Disconnect the Modem from the PC and ADSL Wall Jack (Trennen des Modems vom PC und vom ADSL-Splitter) 13
Abbildung 5-5: Setup-Assistent – Fenster Connect the Gateway to the ADSL Wall Jack (Anschließen des Gateways an den ADSL-Splitter) 14
Abbildung 5-6: Setup-Assistent – Fenster Connect a Network Cable to a PC (Anschließen des Netzwerkkabels an einen PC) 14
Abbildung 5-7: Setup-Assistent – Fenster Connect the Network Cable to the Gateway (Anschließen des Netzwerkkabels an das Gateway) 15
Abbildung 5-8: Setup-Assistent – Fenster Power on the Gateway (Einschalten des Gateways) 15
Abbildung 5-9: Setup-Assistent – Fenster Check the Gateway’s Status (Überprüfen des Gateway-Status) 16
Abbildung 5-10: Setup-Assistent – Fenster Select Your Country (Auswahl des Landes) 16
Abbildung 5-11: Setup-Assistent – Fenster Select Your Internet Service Provider (UK) (Auswahl des Internet-Dienstanbieters in Großbritannien) 17
Abbildung 5-12: Setup-Assistent – Fenster Configure DSL (Konfigurieren von DSL) – „1483 Bridged“ (1483-Überbrückung) 17
Abbildung 5-13: Setup-Assistent – Fenster Configure DSL (Konfigurieren von DSL) – 1483 Routed“ (1483-Weiterleitung) 18
Abbildung 5-14: Setup-Assistent – Fenster Configure DSL (Konfigurieren von DSL) – „PPPoA“ 19
Abbildung 5-15: Setup-Assistent – Fenster Configure DSL (Konfigurieren von DSL) – „PPPoE“ 20

Abbildung 5-16: Setup-Assistent – Fenster Set the Gateway's Password (Einrichten des Gateway-Passworts) 20
Abbildung 5-17: Setup-Assistent – Fenster Wireless Settings (Wireless-Einstellungen) 21
Abbildung 5-18: Setup-Assistent – Fenster Configure Wireless Security Settings (Konfigurieren der Wireless-Sicherheitseinstellungen) 21
Abbildung 5-19: Setup-Assistent – Fenster Wireless Security (Wireless-Sicherheit) – „WPA Personal“ 22
Abbildung 5-20: Setup-Assistent – Fenster Wireless Security (Wireless-Sicherheit) – „WPA2 Personal“ 22
Abbildung 5-21: Setup-Assistent – Fenster Wireless Security (Wireless-Sicherheit) – „WPA2 Mixed Mode“ (WPA2 Gemischter Modus) 23
Abbildung 5-22: Setup-Assistent – Fenster Wireless Security (Wireless-Sicherheit) – WEP (64-Bit)“ 23
Abbildung 5-23: Setup-Assistent – Fenster Wireless Security (Wireless-Sicherheit) – „WEP (128-Bit)“ 24
Abbildung 5-24: Setup-Assistent – Fenster Confirm New Settings (Bestätigen der neuen Einstellungen) 24
Abbildung 5-25: Setup-Assistent – Fenster Safe Surfing (Sicheres Surfen) 25
Abbildung 5-26: Setup-Assistent – Fenster Congratulations (Herzlichen Glückwunsch) 25
Abbildung 6-1: Anmeldefenster 29
Abbildung 6-2: „Basic Setup“ (Grundlegende Einrichtung) 29
Abbildung 6-3: „RFC 1483 Bridged“ (RFC 1483-Überbrückung) 30
Abbildung 6-4: „RFC 1483 Routed“ (RFC 1483-Weiterleitung) 31
Abbildung 6-5: IPoA 31
Abbildung 6-6: RFC 2516 PPPoE 32
Abbildung 6-7: RFC 2364 PPPoA 32
Abbildung 6-8: „Bridge Mode Only“ (Nur Überbrückungsmodus) 33
Abbildung 6-9: „Optional Settings“ (Optionale Einstellungen) 33
Abbildung 6-10: DDNS – DynDNS.org 35
Abbildung 6-11: DDNS – TZO.com 35
Abbildung 6-12: „Advanced Routing“ (Erweitertes Routing) 36
Abbildung 6-13: „Routing Table“ (Routing-Tabelle) 37
Abbildung 6-14: „Basic Wireless Settings“ (Grundlegende Wireless-Einstellungen) 38
Abbildung 6-15: „Wireless Security“ (Wireless-Sicherheit) – „WPA-Personal“ 39

Abbildung 6-16: „Wireless Security“ (Wireless-Sicherheit) – „WPA2-Personal“ 39
Abbildung 6-17: „Wireless Security“ (Wireless-Sicherheit) – „WPA2-Mixed“ (WPA2 Gemischt) 40
Abbildung 6-18: „Wireless Security“ (Wireless-Sicherheit) – „WPA Enterprise“ 40
Abbildung 6-19: „Wireless Security“ (Wireless-Sicherheit) – „WPA2 Enterprise“ 41
Abbildung 6-20: „Wireless Security“ (Wireless-Sicherheit) – „WEP“ 41
Abbildung 6-21: „Wireless Access“ (Wireless-Zugriff) 42
Abbildung 6-22: „MAC Address Filter List“ (MAC-Adressen-Filterliste) 42
Abbildung 6-23: „Wireless Client MAC List“ (MAC-Liste der Wireless-Clients) 42
Abbildung 6-24: „Advanced Wireless Settings“ (Erweiterte Wireless-Einstellungen) 43
Abbildung 6-25: Firewall 45
Abbildung 6-26: „VPN Passthrough“ (VPN-Passthrough) 46
Abbildung 6-27: VPN 47
Abbildung 6-28: „VPN Settings Summary“ (Zusammenfassung der VPN-Einstellungen) 47
Abbildung 6-29: „Key Exchange Method“ (Methode für den Schlüsselaustausch) – „Auto (IKE)“ 48
Abbildung 6-30: „Key Exchange Method“ (Methode für den Schlüsselaustausch) – „Manual“ (Manuell) 49
Abbildung 6-31: „VPN Log“ (VPN-Protokoll) 50
Abbildung 6-32: „Advanced VPN Tunnel Setup“ (Erweiterte IPSec VPN-Tunnel-Einrichtung) 51
Abbildung 6-33: „Internet Access Policy“ (Richtlinien für Internetzugriff) 53
Abbildung 6-34: „Internet Policy Summary“ (Internetrichtlinien – Zusammenfassung) 53
Abbildung 6-35: „List of PCs“ (PC-Liste) 54
Abbildung 6-36: „Single Port Forwarding“ (Einfache Anschlussweiterleitung) 55
Abbildung 6-37: „Port Range Forwarding“ (Weiterleitung an einen Anschlussbereich) 56
Abbildung 6-38: „Port Rage Triggering“ (Anschlussbereich-Triggering) 57
Abbildung 6-39: DMZ 58
Abbildung 6-40: QoS 59
Abbildung 6-41: QoS – „Online Game“ (Online-Spiel) 60
Abbildung 6-42: QoS – MSN Messenger 60
Abbildung 6-43: QoS – „Voice Device“ (Sprachgerät) 60
Abbildung 6-44: QoS – „Add a New Application“ (Neue Anwendung hinzufügen) – „Port Range“ (Anschlussbereich) 60
Abbildung 6-45: QoS – „Add a New Application“ (Neue Anwendung hinzufügen) – „MAC Address“ (MAC-Adresse) 61
Abbildung 6-46: „Management“ (Verwaltungsfunktionen) 62

Abbildung 6-47: „Allowed IP“ (Zugelassene IP) – „IP Range“ (IP-Bereich) 62
Abbildung 6-48: „Reporting“ (Berichtaufzeichnung) 64
Abbildung 6-49: „System Log“ (Systemprotokoll) 64
Abbildung 6-50: „Diagnostics“ (Diagnose) 65
Abbildung 6-51: „Backup&Restore“ (Sichern & Wiederherstellen) 65
Abbildung 6-52: „Factory Defaults“ (Werkseinstellungen) 66
Abbildung 6-53: „Firmware Upgrade“ (Aktualisieren der Firmware) 66
Abbildung 6-54: Gateway 67
Abbildung 6-55: „Local Network“ Lokales Netzwerk 68
Abbildung 6-56: DHCP – „DHCP Active IP Table“ (Tabelle zur aktiven IP-Adresse) 68
Abbildung 6-57: „ARP/RARP Table“ (ARP/RARP-Tabelle) 68
Abbildung 6-58: Wireless 69
Abbildung 6-59: „Networked Computers“ (Netzwerk-Computer) 69
Abbildung 6-60: „DSL Connection“ (DSL-Verbindung) 70
Abbildung C-1: IP-Konfiguration 92
Abbildung C-2: MAC-Adresse/Adapteradresse 92
Abbildung C-3: MAC-Adresse/physische Adresse 93
Abbildung D-1: Aktualisieren der Firmware 94

# Kapitel 1: Einführung

## Willkommen

Vielen Dank, dass Sie sich für ein Wireless-G ADSL-Gateway mit SRX200 entschieden haben. Mit diesem Gateway stehen den Computern eine High Speed-Internetverbindung und Ressourcen wie beispielsweise Dateien und Drucker zur Verfügung.

Wie schafft das Gateway das? Wenn das Gateway mit dem Internet sowie Computern und Peripheriegeräten verbunden wird, kann die Netzwerkkommunikation durch das Gateway gesteuert und überwacht werden. Und da es sich um ein Wireless-Gateway handelt, kann der Internetzugriff sowohl als Wireless-Übertragung als auch über das verdrahtete Netzwerk erfolgen.

Der Wireless-G ADSL-Gateway mit SRX200 kombiniert eine neue Antennentechnologie mit dem standardisierten Wireless-G (802.11g)-Netzwerkbetrieb. Die hier verwendete MIMO-Technologie (*Multiple Inputs - Multiple Outputs*) überlagert die Signale zweier Wireless-G-kompatibler Funkgeräte und verdoppelt so praktisch die Datenrate. Im Gegensatz zu den üblichen Wireless-Netzwerktechnologien, bei denen sich Signalreflexionen störend auswirken, verwendet die MIMO-Technologie diese Reflexionen, um die Reichweite zu erhöhen und tote Punkte im Wireless-Empfangsbereich zu beseitigen. Das robuste Signal hat eine größere Reichweite, so dass in Wireless-Verbindungen über bis zu zweimal höhere Entfernungen aufrechterhalten werden können als bei standardmäßigen Wireless-G-Systemen. Je größer die Entfernung, desto größer der Vorteil: Mit der höheren Datenrate und der reflexionsresistenten Technologie lässt sich in manchen Situationen ein bis zu sechsmal höherer Durchsatz erzielen als bei Wireless-G. Interferenzen werden dadurch vermieden, dass das Gateway dynamisch zum Kanal mit dem deutlichsten Signal wechselt. Auch bei standardmäßigen Wireless-G- und Wireless-B-Systemen lässt sich die Leistung verbessern, wenn diese mit SRX-fähigen Geräten kommunizieren.

Zum Schutz der Daten und der Privatsphäre bietet die WEP-Verschlüsselung darüber hinaus bessere Sicherheitsoptionen, während das gesamte Netzwerk durch die SPI-Firewall (*Stateful Packet Inspection*) und NAT-Technologie geschützt ist. Zudem können Sie Ihre Familie mit Kinderschutzfunktionen wie dem Einschränken der Internetzugriffszeiten und dem Blockieren von Schlüsselwörtern schützen. Der Zugriff auf diese Sicherheitsfunktionen sowie auf die anderen Einstellungen des Gateways erfolgt über ein benutzerfreundliches, browserbasiertes Dienstprogramm.

Und was genau bedeutet das?

***802.11b**: IEEE-Standard für den Wireless-Netzwerkbetrieb, der eine maximale Datenübertragungsrate von 11 MBit/s sowie eine Betriebsfrequenz von 2,4 GHz festlegt.*

***802.11g**: IEEE-Standard für den Wireless-Netzwerkbetrieb, der eine maximale Datenübertragungsrate von 54 MBit/s und eine Betriebsfrequenz von 2,4 GHz festlegt sowie Abwärtskompatibilität mit Geräten garantiert, die dem Standard 802.11b entsprechen.*

***WPA** (Wi-Fi Protected Access): Ein Wireless-Sicherheitsprotokoll, bei dem eine TKIP-Verschlüsselung (Temporal Key Integrity Protocol) verwendet wird, die zusammen mit einem RADIUS-Server eingesetzt werden kann.*

***SPI-Firewall** (Stateful Packet Inspection): Eine Technologie zur Überprüfung von eingehenden Datenpaketen, bevor diese an das Netzwerk weitergeleitet werden.*

***Firewall**: Sicherheitsmaßnahmen, durch die die Ressourcen in einem lokalen Netzwerk vor dem Zugriff durch nicht autorisierte Dritte geschützt werden.*

***NAT** (Network Address Translation): Die NAT-Technologie übersetzt IP-Adressen von lokalen Netzwerken in eine andere IP-Adresse für das Internet.*

Mit Netzwerken können Sie einen Internetzugang und Computer-Ressourcen gemeinsam mit anderen nutzen. Sie können von verschiedenen Computern aus auf einem Drucker drucken und auf Daten zugreifen, die auf der Festplatte eines anderen Computers gespeichert sind. Netzwerke eignen sich darüber hinaus auch für Videospiele mit mehreren Spielern. Netzwerke sind also nicht nur zu Hause und im Büro nützlich, sondern lassen sich auch für Unterhaltungszwecke nutzen.

Mehrere PCs in einem verdrahteten Netzwerk stellen ein LAN (*Local Area Network*; Lokales Netzwerk) dar. Sie werden über Ethernetkabel angeschlossen, daher die Bezeichnung „verdrahtetes“ Netzwerk. Mit Wireless-Karten oder -Adaptern ausgerüstete PCs können ganz ohne lästige Kabel kommunizieren. Indem sie innerhalb ihres Übertragungsradius dieselben Wireless-Einstellungen verwenden, bilden sie ein Wireless-Netzwerk. Dies wird oft als WLAN oder *Wireless Local Area Network* (drahtloses lokales Netzwerk) bezeichnet. Da das Gateway mit Wireless-Funktionen ausgestattet ist, können verdrahtete Netzwerke und Wireless-Netzwerke miteinander verbunden werden, sodass sie miteinander kommunizieren können.

Durch das Verbinden aller verdrahteten und Wireless-Netzwerke sowie des Internets können Sie jetzt Dateien gemeinsam verwenden, auf das Internet zugreifen und sogar Spiele spielen. Dabei schützt der Wireless-G ADSL-Gateway mit SRX200 die Netzwerke stets vor nicht autorisierten und nicht willkommenen Benutzern.

Linksys empfiehlt die Verwendung der Installations-CD-ROM zur erstmaligen Installation des Gateways. Wenn Sie den Setup-Assistenten auf der Installations-CD-ROM nicht ausführen möchten, können Sie das Gateway anhand der Anweisungen in diesem Handbuch anschließen, einrichten und für die Verbindung mit den verschiedenen Netzwerken konfigurieren. Diese Anweisungen enthalten alle Informationen, die Sie zur optimalen Nutzung des Wireless-G ADSL-Gateways mit SRX200 benötigen.

***Netzwerk**: Mehrere Computer oder Geräte, die miteinander verbunden sind, damit Benutzer Daten gemeinsam verwenden, speichern und miteinander austauschen können.*

***LAN** (Local Area Network): Die Computer und Netzwerkbetriebsprodukte, aus denen sich Ihr Heim- oder Büronetzwerk zusammensetzt.*

## Inhalt dieses Benutzerhandbuchs

In diesem Benutzerhandbuch sind die zur Installation und Verwendung des Wireless-G ADSL-Gateways mit SRX200 erforderlichen Schritte aufgeführt.

- Kapitel 1: Einführung
  In diesem Kapitel werden die Anwendungen des Wireless-G ADSL-Gateways mit SRX200 sowie dieses Benutzerhandbuch beschrieben.

- Kapitel 2: Planen des Netzwerks
  In diesem Kapitel werden die Grundlagen des Netzwerkbetriebs beschrieben.

- Kapitel 3: Beschreibung des Wireless-G ADSL-Gateways mit SRX200
  In diesem Kapitel werden die physischen Merkmale des Gateways beschrieben.

- Kapitel 4: Anschließen des Wireless-G Broadband-Gateways mit SRX200
  In diesem Kapitel finden Sie Anleitungen zum Anschließen des Gateways an Ihr Netzwerk.

- Kapitel 5: Einrichten des Wireless-G ADSL-Gateways mit SRX200
  In diesem Kapitel wird das Einrichten des Gateways mit dem Setup-Assistenten beschrieben.

- Kapitel 6: Konfigurieren des Wireless-G Broadband-Gateways mit SRX200
  In diesem Kapitel wird beschrieben, wie Sie die Einstellungen des Gateways mithilfe des webbasierten Dienstprogramms konfigurieren.

- Anhang A: Fehlerbehebung
  In diesem Anhang werden einige Probleme und Lösungsansätze sowie häufig gestellte Fragen im Zusammenhang mit der Installation und Verwendung des Wireless-G ADSL-Gateways mit SRX200 erörtert.

- Anhang B: Wireless-Sicherheit
  In diesem Anhang werden die Risiken des Wireless-Netzwerkbetriebs sowie einige Lösungen zur Eingrenzung der Risiken erklärt.

- Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters
  In diesem Anhang wird beschrieben, wie Sie die MAC-Adresse für den Ethernet-Adapter des Computers ermitteln, um die MAC-Filterung bzw. die Gateway-Funktion zum Kopieren von MAC-Adressen verwenden zu können.

- Anhang D: Aktualisieren der Firmware
  In diesem Anhang finden Sie eine Anleitung zum Aktualisieren der Firmware des Gateways, sollte dies einmal erforderlich sein.

- Anhang E: Glossar
  In diesem Anhang finden Sie ein kurzes Glossar mit häufig verwendeten Begriffen aus dem Bereich Netzwerkbetrieb.

- Anhang F: Spezifikationen
  In diesem Anhang sind die technischen Spezifikationen des Gateways aufgeführt.

- Anhang G: Garantieinformationen
  Dieser Anhang enthält die Garantieinformationen für das Gateway.

- Anhang H: Zulassungsinformationen
  Dieser Anhang enthält die für das Gateway geltenden Zulassungsinformationen.

- Anhang I: Kontaktinformationen
  In diesem Anhang finden Sie Kontaktinformationen zu einer Reihe von Linksys Ressourcen, darunter auch zum Support.

# Kapitel 2: Planen des Netzwerks

## Funktionen des Gateways

Ein Gateway ist ein Netzwerkgerät, das zwei Netzwerke miteinander verbindet.

In diesem Fall verbindet das Gateway das lokale Netzwerk (LAN) oder die Computer zu Hause oder im Büro mit dem Internet. Das Gateway verarbeitet und lenkt die zwischen diesen beiden Netzwerken übertragenen Daten.

Mit der NAT-Funktion des Gateways wird das Computernetzwerk geschützt, sodass Ihre Computer für andere Benutzer im Internet nicht „sichtbar" sind. Somit wird der private Charakter des Netzwerks bewahrt. Das Gateway schützt das Netzwerk, indem es alle über den Internet-Port eingehenden Datenpakete überprüft, bevor sie an den entsprechenden Computer in Ihrem Netzwerk geliefert werden. Das Gateway überprüft Internet-Anschlussdienste, wie z. B. den Webserver, FTP-Server oder andere Internetanwendungen, und leitet, falls zulässig, das jeweilige Paket an den entsprechenden Computer im LAN weiter.

Beachten Sie, dass über die Ports des Gateways eine Verbindung zwischen zwei Netzwerken hergestellt wird. Mit den LAN-Ports können Sie Verbindungen zum LAN und mit dem Port **ADSL** eine Verbindung zum Internet herstellen. Die LAN-Ports übertragen Daten mit einer Geschwindigkeit von 10/100 Mbit/s.

**Abbildung 2-1: Netzwerk**

## IP-Adressen

### Was ist eine IP-Adresse?

IP steht für *Internet Protocol* (Internet-Protokoll). Jedes Gerät in einem IP-basierten Netzwerk, einschließlich Computern, Druckservern und Gateways, benötigt eine IP-Adresse, mit der sein „Standort" bzw. seine Adresse im Netzwerk identifiziert werden kann. Dies gilt sowohl für Internet- als auch für LAN-Verbindungen. Es gibt zwei Möglichkeiten, den Netzwerkgeräten eine IP-Adresse zuzuweisen. Sie können statische IP-Adressen oder mithilfe des Gateways dynamische IP-Adressen zuweisen.

### Statische IP-Adressen

Bei einer statischen IP-Adresse handelt es sich um eine feste IP-Adresse, die einem Computer oder einem anderen Netzwerkgerät manuell zugewiesen wird. Da eine statische IP-Adresse solange gültig ist, bis Sie sie deaktivieren, wird durch das Zuweisen einer statischen IP-Adresse sichergestellt, dass das entsprechende Gerät stets dieselbe IP-Adresse hat, bis diese geändert wird. Statische IP-Adressen müssen eindeutig sein und werden im Allgemeinen bei Netzwerkgeräten, z. B. Server-Computern oder Druckservern, verwendet.

***IP** (Internet Protocol): Ein Protokoll zum Senden von Daten über Netzwerke.*

**HINWEIS:** Da es sich bei dem Gateway um ein Gerät handelt, mit dem zwei Netzwerke verbunden werden, sind zwei IP-Adressen erforderlich, eine für das LAN und eine für das Internet. In diesem Benutzer-handbuch wird auf „Internet-IP-Adressen" und „LAN-IP-Adressen" verwiesen.

Da bei dem Gateway NAT-Technologie eingesetzt wird, ist die einzige IP-Adresse Ihres Netzwerks, die vom Internet aus sichtbar ist, die Internet-IP-Adresse des Gateways. Es kann jedoch auch diese Internet-IP-Adresse blockiert werden, so dass Gateway und Netzwerk für das Internet unsichtbar sind. Weitere Informationen hierzu finden Sie in „Kapitel 6: Konfigurieren des Wireless-G ADSL-Gateways mit SRX200" im Abschnitt zur Registerkarte **Security – Firewall** (Sicherheit – Firewall).

Da Sie das Gateway für den gemeinsamen Zugriff auf Ihre DSL-Internetverbindung verwenden, fragen Sie Ihren ISP, ob Ihrem Konto eine statische IP-Adresse zugewiesen wurde. Ist dies der Fall, benötigen Sie diese statische IP-Adresse für die Konfiguration des Gateways. Sie erhalten diese Informationen von Ihrem ISP.

## Dynamische IP-Adressen

Eine dynamische IP-Adresse wird einem Netzwerkgerät, z. B. einem Computer oder Druckserver, automatisch zugewiesen. Diese IP-Adressen werden als „dynamisch“ bezeichnet, da sie den Netzwerkgeräten nur vorübergehend zugewiesen werden. Nach einem bestimmten Zeitraum laufen Sie ab und können geändert werden. Wenn ein Computer beim Netzwerk (oder im Internet) angemeldet wird und seine dynamische IP-Adresse abgelaufen ist, wird ihm vom DHCP-Server automatisch eine neue dynamische IP-Adresse zugewiesen.

## DHCP-Server (*Dynamic Host Configuration Protocol*)

Computern und anderen Netzwerkgeräten mit dynamischen IP-Adressen wird von einem DHCP-Server jeweils eine neue IP-Adresse zugewiesen. Computer bzw. Netzwerkgeräte, die eine IP-Adresse erhalten, werden als DHCP-Clients bezeichnet. Durch DHCP müssen Sie nicht jedes Mal, wenn dem Netzwerk ein neuer Benutzer hinzugefügt wird, manuell eine IP-Adresse zuweisen.

Als DHCP-Server kann entweder ein bestimmter Computer im Netzwerk oder ein anderes Netzwerkgerät (z. B. das Gateway) fungieren. Die DHCP-Serverfunktion des Gateways ist standardmäßig aktiviert.

Wenn im Netzwerk bereits ein DHCP-Server ausgeführt wird, müssen Sie einen der beiden DHCP-Server deaktivieren. Wenn mehrere DHCP-Server in Ihrem Netzwerk ausgeführt werden, treten Netzwerkfehler (z. B. IP-Adresskonflikte) auf. Hinweise zum Deaktivieren von DHCP für das Gateway finden Sie in „Kapitel 6: Konfigurieren des Wireless-G ADSL-Gateways mit SRX200“ im Abschnitt „DHCP“.

# Kapitel 3: Beschreibung des Wireless-G ADSL-Gateways mit SRX200

## Ports und Taste „Reset“ an der Geräteseite

Die Ports und die Taste **Reset** befinden sich an der Geräteseite des Gateways.

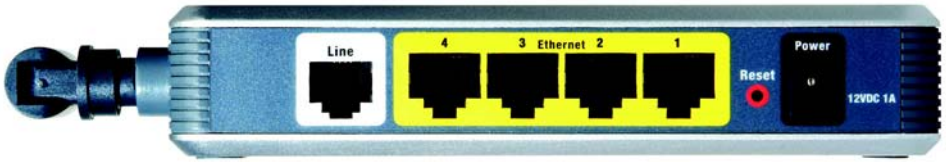


**Abbildung 3-1: Ports und Taste „Reset“ an der Geräteseite**

**Line** (Verbindung) Der Port **Line** (Verbindung) dient zum Anschließen an die ADSL-Verbindung.

**Ethernet (1-4)** Die **Ethernet**-Ports dienen zum Anschließen an die Computer und andere Netzwerkgeräte.

**Reset** (Taste) Das Gateway kann auf zweierlei Weise auf die Werkseinstellungen zurückgesetzt werden. Halten Sie die Taste **Reset** ungefähr fünf Sekunden lang gedrückt, oder setzen Sie die Einstellungen im webbasierten Dienstprogramm des Gateways auf der Registerkarte **Administration** (Verwaltung) im Fenster *Factory Defaults* (Werkseinstellungen) zurück.

**Power** (Netzstrom) Der Port **Power** (Netzstrom) dient zum Anschließen des Netzstromadapters.

**WICHTIG:** Durch das Zurücksetzen des Gateways auf die Werkseinstellungen werden alle Einstellungen gelöscht (einschließlich der Einstellungen für die Internetverbindung, der Wireless-Einstellungen und anderer Einstellungen) und durch die Werkseinstellungen ersetzt. Setzen Sie das Gateway nicht zurück, wenn Sie die Einstellungen beibehalten möchten.

## LEDs an der Geräteseite

Die LEDs des Gateways, die Netzwerkaktivität anzeigen, befinden sich an der anderen Geräteseite.

**Abbildung 3-2: LEDs an der Geräteseite**

**Ein/Aus** (Taste) Drücken Sie diese Taste, wenn Sie das Gateway ein- oder ausschalten möchten.

**POWER** (Netzstrom) Grün. Die LED **POWER** (Netzstrom) leuchtet, wenn das Gateway eingeschaltet wird.

**WIRELESS** Grün. Die LED **WIRELESS** leuchtet bei jeder erfolgreichen Wireless-Verbindung. Wenn die LED blinkt, werden gerade aktiv Daten vom Gateway an eines der Netzwerkgeräte gesendet oder es werden gerade Daten empfangen.

**ETHERNET (1-4)** Grün. Die LED **ETHERNET** hat zwei Funktionen. Wenn die LED durchgängig leuchtet, ist das Gateway erfolgreich über den entsprechenden Ethernet-Port mit einem Gerät verbunden. Wenn die LED blinkt, finden Netzwerkaktivitäten statt.

**DSL** Grün. Die LED **DSL** leuchtet bei jeder erfolgreichen DSL-Verbindung. Die LED blinkt, wenn mit dem Gateway eine ADSL-Verbindung hergestellt wurde.

**INTERNET** Grün. Die LED **INTERNET** leuchtet grün, wenn eine Internetverbindung zum Internet-Dienstanbieter (ISP) hergestellt wurde. Die LED leuchtet rot, wenn bei der Verbindung zum ISP Fehler auftreten.

# Kapitel 4: Anschließen des Wireless-G ADSL-Gateways mit SRX200

## Übersicht

In der Regel erhalten Sie vom Installationstechniker Ihres Internet-Dienstanbieters (ISP) nach der Installation der Breitbandverbindung Informationen zur Einrichtung des Modems. Wenn diese Daten nicht zur Verfügung stehen, fordern Sie sie von Ihrem ISP an.

Wenn Sie über die für Ihren Internetverbindungstyp erforderlichen Einrichtungsinformationen verfügen, können Sie mit der Installation und Einrichtung des Gateways beginnen.

Wenn Sie zur Konfiguration des Gateways einen Computer mit einem Ethernet-Adapter verwenden möchten, fahren Sie mit Abschnitt „Verdrahtete Verbindung mit einem Computer“ fort. Wenn Sie zur Konfiguration des Gateways einen Computer mit einem Wireless-Adapter verwenden möchten, fahren Sie mit Abschnitt „Wireless-Verbindung mit einem Computer“ fort.

## Verdrahtete Verbindung mit einem Computer

1. Stellen Sie sicher, dass alle Hardwaregeräte des Netzwerks (einschließlich des Gateways und der Computer) ausgeschaltet sind.

2. Schließen Sie ein Ende des Telefonkabels an den Port **Line** (Verbindung) an der Geräteseite des Gateways an und das andere Ende an den Splitter der ADSL-Leitung. Um Störungen zu vermeiden, muss u. U. zwischen Telefon und Splitter ein so genannter Mikrofilter (nicht im Lieferumfang enthalten) geschaltet werden. Sollten Sie Fragen hierzu haben, wenden Sie sich an Ihren ISP.

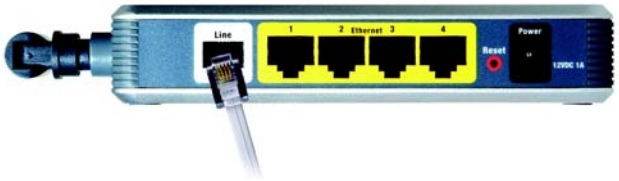


**Abbildung 4-1: Herstellen der ADSL-Verbindung**

**HINWEIS:** Um Störungen zu vermeiden, muss u. U. zwischen Telefon und Splitter ein so genannter Mikrofilter (nicht im Lieferumfang enthalten) geschaltet werden. Sollten Sie Fragen hierzu haben, wenden Sie sich an Ihren ISP.

**WICHTIG:** Vergewissern Sie sich in Ländern, in denen Telefonbuchsen mit RJ-11-Steckern verwendet werden, dass Sie die Mikrofilter nur zwischen das Telefon und den Splitter und **nicht** zwischen das Gateway und den Splitter schalten. Andernfalls kann keine ADSL-Verbindung hergestellt werden.

In Ländern, in denen **keine** Telefonbuchsen mit RJ-11-Steckern verwendet werden (z. B. Frankreich, Schweden, Schweiz, Großbritannien), muss der Mikrofilter – mit Ausnahme von ISDN – zwischen das Gateway und die Wandbuchse geschaltet werden, da sich der RJ-11-Stecker am Mikrofilter befindet.

Benutzer von Annex B (Gateway-Versionen E1 und DE) verwenden zum Anschließen des Gateways an den Splitter oder den NTBA das im Lieferumfang enthaltene Netzwerkkabel. Wenn Sie Splitter oder spezielle Stecker benötigen, wenden Sie sich an Ihren Internet-Dienstanbieter.

3. Schließen Sie ein Ende des Ethernet-Netzwerkkabels an einen der Ethernet-Ports (mit 1-4 beschriftet) an der Geräteseite des Gateways und das andere Ende am Ethernet-Port eines Computers an.

   Wiederholen Sie diesen Schritt, um weitere Computer, einen Switch oder andere Netzwerkgeräte an das Gateway anzuschließen.

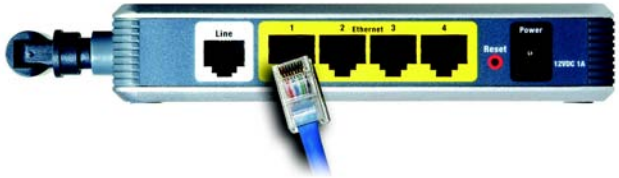


**Abbildung 4-2: Anschließen eines PCs**

4. Schließen Sie den Netzstromadapter an den Port **Power** (Netzstrom) des Gateways an, und stecken Sie ihn anschließend in eine Steckdose.

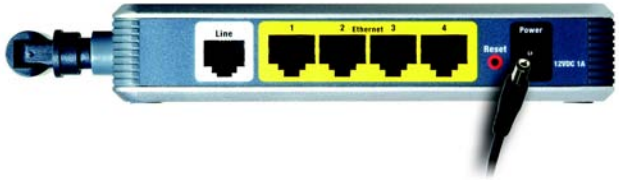


**Abbildung 4-3: Anschließen des Netzstroms**

**HINWEIS:** Schließen Sie den Netzstromadapter des Gateways nur an eine Stromleiste mit Überspannungsschutz an.

Wenn der Netzstromadapter ordnungsgemäß angeschlossen ist, leuchtet die LED **Power** (Netzstrom) an der Geräteseite grün. Die LED **Power** (Netzstrom) blinkt einige Sekunden lang und leuchtet konstant, nachdem die Selbstdiagnose abgeschlossen wurde. Wenn die LED länger als eine Minute blinkt, finden Sie entsprechende Informationen zur Fehlerbehebung in „Anhang A: Fehlerbehebung“.

5. Schalten Sie einen Computer ein, der mit dem Gateway verbunden ist.

**Fahren Sie mit „Kapitel 5: Einrichten des Wireless-G ADSL-Gateways mit SRX200“ fort.**

## Wireless-Verbindung mit einem Computer

Befolgen Sie die nachstehenden Anweisungen, wenn Sie über eine Wireless-Verbindung auf das Gateway zugreifen möchten:

1. Stellen Sie sicher, dass alle Hardwaregeräte des Netzwerks (einschließlich des Gateways und der Computer) ausgeschaltet sind.

2. Schließen Sie ein Ende des Telefonkabels an den Port **Line** (Verbindung) an der Rückseite des Gateways an und das andere Ende an die Wandbuchse der ADSL-Leitung. Um Störungen zu vermeiden, muss u. U. zwischen Telefon und Splitter ein so genannter Mikrofilter (nicht im Lieferumfang enthalten) geschaltet werden. Sollten Sie Fragen hierzu haben, wenden Sie sich an Ihren ISP.

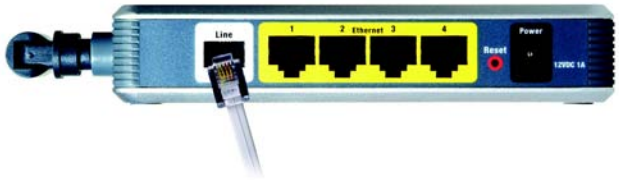


**Abbildung 4-4: Herstellen der ADSL-Verbindung**

**HINWEIS:** Um Störungen zu vermeiden, muss u. U. zwischen Telefon und Splitter ein so genannter Mikrofilter (nicht im Lieferumfang enthalten) geschaltet werden. Sollten Sie Fragen hierzu haben, wenden Sie sich an Ihren ISP.

**WICHTIG:** Vergewissern Sie sich in Ländern, in denen Telefonbuchsen mit RJ-11-Steckern verwendet werden, dass Sie die Mikrofilter nur zwischen das Telefon und den Splitter und **nicht** zwischen das Gateway und den Splitter schalten. Andernfalls kann keine ADSL-Verbindung hergestellt werden.

In Ländern, in denen **keine** Telefonbuchsen mit RJ-11-Steckern verwendet werden (z. B. Frankreich, Schweden, Schweiz, Großbritannien), muss der Mikrofilter – mit Ausnahme von ISDN – zwischen das Gateway und die Wandbuchse geschaltet werden, da sich der RJ-11-Stecker am Mikrofilter befindet.

Benutzer von Annex B (Gateway-Versionen E1 und DE) verwenden zum Anschließen des Gateways an den Splitter oder den NTBA das im Lieferumfang enthaltene Netzwerkkabel. Wenn Sie Splitter oder spezielle Stecker benötigen, wenden Sie sich an Ihren Internet-Dienstanbieter.

3. Schließen Sie den Netzstromadapter an den Port **Power** (Netzstrom) an, und stecken Sie ihn anschließend in eine Steckdose.

**HINWEIS:** Schließen Sie den Netzstromadapter des Gateways nur an eine Stromleiste mit Überspannungsschutz an.

Wenn der Netzstromadapter ordnungsgemäß angeschlossen ist, leuchtet die LED **Power** (Netzstrom) an der Geräteseite grün. Die LED **Power** (Netzstrom) blinkt einige Sekunden lang und leuchtet konstant, nachdem die Selbstdiagnose abgeschlossen wurde. Wenn die LED länger als eine Minute blinkt, finden Sie entsprechende Informationen zur Fehlerbehebung in „Anhang A: Fehlerbehebung“.

4. Schalten Sie einen der Computer im Wireless-Netzwerk ein.

5. Stellen Sie beim erstmaligen Zugriff auf das Gateway über eine Wireless-Verbindung sicher, dass die SSID des Wireless-Adapters für den Computer auf **linksys** (die Standardeinstellung des Gateways) eingestellt und die Option zur Sicherheit im Wireless-Netzwerkbetrieb deaktiviert ist. Wenn Sie Zugriff auf das Gateway haben, können Sie die Einstellungen des Gateways und des Adapters für den Computer an die üblichen Netzwerkeinstellungen anpassen.

**Fahren Sie mit „Kapitel 5: Einrichten des Wireless-G ADSL-Gateways mit SRX200“ fort.**

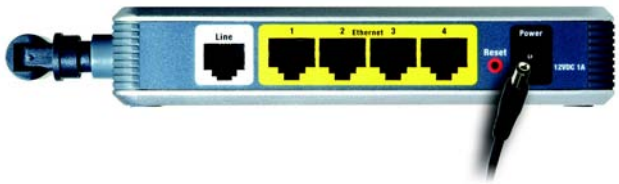


**Abbildung 4-5: Anschließen des Netzstroms**

**HINWEIS:** Sie sollten auf jeden Fall die SSID-Standardeinstellung **linksys** ändern und die Option zur Sicherheit im Wireless-Netzwerkbetrieb aktivieren.

# Kapitel 5: Einrichten des Wireless-G ADSL-Gateways mit SRX200

## Übersicht

Der Setup-Assistent für das Wireless-G ADSL-Gateway mit SRX200 führt Sie durch den Installationsvorgang. Er zeigt Ihnen Schritt für Schritt auf, wie Sie die Netzwerk- und Wireless-Einstellungen des Gateways konfigurieren.

## Verwenden des Setup-Assistenten

1. Legen Sie die **Setup Wizard CD-ROM** (Setup-Assistenten-CD-ROM) in Ihr CD-ROM-Laufwerk ein. Der Setup-Assistent sollte automatisch gestartet und das Willkommensfenster angezeigt werden. Ist dies nicht der Fall, klicken Sie auf die Schaltfläche **Start**, und wählen Sie **Ausführen** aus. Geben Sie im daraufhin angezeigten Feld **D:\setup.exe** ein (wobei „D“ für den Buchstaben des CD-ROM-Laufwerks steht).

2. Die Spracheinstellung des Computers wird vom Setup-Assistenten automatisch erkannt. Ist dies nicht der Fall, wählen Sie eine der verfügbaren Sprachen im Dropdown-Menü *Language* (Sprache) aus. Klicken Sie im ersten Willkommensfenster auf die Schaltfläche **Next** (Weiter), wenn Sie den Setup-Assistenten in der aktuellen Sprache ausführen möchten. Wenn Sie eine andere Sprache verwenden möchten, wählen Sie die entsprechende Sprache aus, und klicken Sie dann auf die Schaltfläche **Next** (Weiter).

3. Klicken Sie im nächsten Willkommensfenster auf die Schaltfläche **Click Here to Start** (Klicken Sie hier, um zu starten). Darüber hinaus stehen Ihnen folgende Wahlmöglichkeiten zur Verfügung:

   **Norton Internet Security**: Klicken Sie auf die Schaltfläche **Norton Internet Security**, um das Softwareprogramm Norton Internet Security zu installieren.

   **User Guide** (Benutzerhandbuch): Klicken Sie auf diese Schaltfläche, um das Benutzerhandbuch als PDF-Datei zu öffnen.

   **Exit** (Beenden): Klicken Sie auf diese Schaltfläche, um den Setup-Assistenten zu beenden.

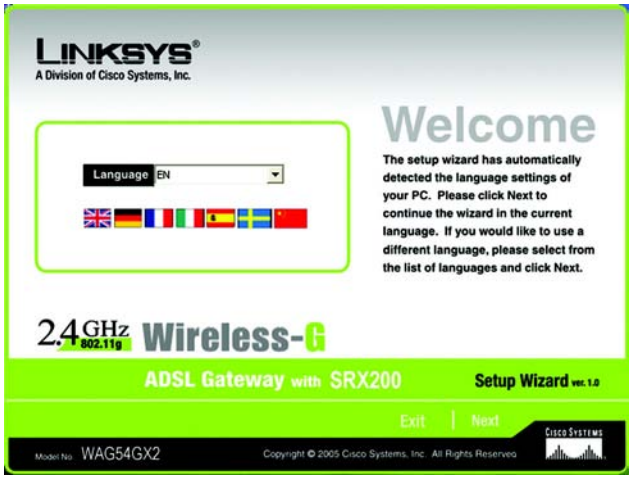
LINKSYS
A Division of Cisco Systems, Inc.
Welcome
Language EN
The setup wizard has automatically detected the language settings of your PC. Please click Next to continue the wizard in the current language. If you would like to use a different language, please select from the list of languages and click Next.
2.4GHz 802.11g Wireless-G
ADSL Gateway with SRX200
Setup Wizard ver. 1.0
Exit
Next
Model No. WAG54GX2
Copyright © 2005 Cisco Systems, Inc. All Rights Reserved
Cisco Systems

**Abbildung 5-1: Setup-Assistent – Willkommensfenster – Sprachauswahl**

LINKSYS
A Division of Cisco Systems, Inc.
Welcome
Thank you for choosing Linksys. This Setup Wizard will help you install the Wireless-G ADSL Gateway with SRX200.
Click Here to Start
2.4GHz 802.11g Wireless-G
SRX200
ADSL Gateway with SRX200
Setup Wizard ver. 1.0
Norton Internet Security
User Guide
Exit
Model No. WAG54GX2
Copyright © 2005 Cisco Systems, Inc. All Rights Reserved
Cisco Systems

**Abbildung 5-2: Setup-Assistent – Willkommensfenster – Fenster zum Starten des Assistenten**

4. Klicken Sie nach dem Lesen der Lizenzvereinbarung auf die Schaltfläche **Next** (Weiter), wenn Sie diese akzeptieren, oder auf die Schaltfläche **Exit** (Beenden), um den Installationsvorgang zu beenden. Klicken Sie auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

LINKSYS®
A Division of Cisco Systems, Inc.
End User License Agreement
1
Please review the license agreement below.
Press the PAGE DOWN key or use the Scroll Bar to see the rest of the agreement.
Linksys Software License Agreement v.8.15.03
THIS LICENSE AGREEMENT IS BETWEEN YOU AND CISCO-LINKSYS, LLC OR THE CISCO-LINKSYS, LLC SUBSIDIARY LICENSING THIS SOFTWARE, IF SALE IS NOT DIRECLTY BY CISCO-LINKSYS, LLC ("Linksys"). BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE PRODUCT CONTAINING THE SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THESE TERMS, THEN YOU MAY NOT
If you accept the terms of this Agreement, click Next to continue. If not, choose Cancel and the Setup Wizard will close. You must click Next to continue the installation process.
Exit | Back | Next
Wireless-G ADSL Gateway with SRX200 Setup Wizard Model No. WAG54GX2

**Abbildung 5-3: Setup-Assistent – Fenster *License Agreement* (Lizenzvereinbarung)**

5. Der Setup-Assistent fordert Sie auf, das Breitband-Modem vom Computer und vom ADSL-Splitter zu trennen. Klicken Sie anschließend auf die Schaltfläche **Next** (Weiter).

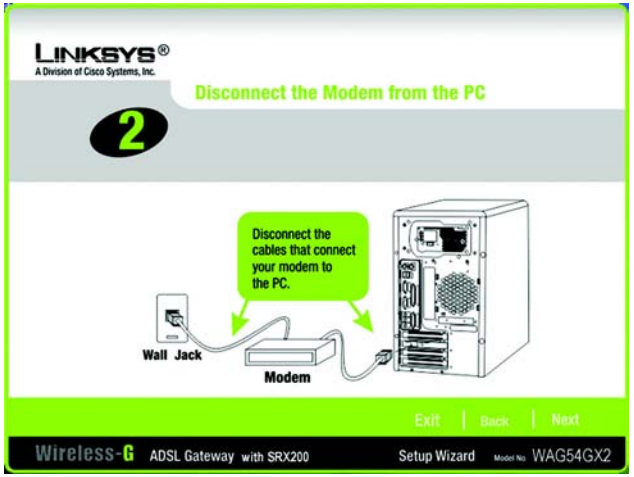
LINKSYS®
A Division of Cisco Systems, Inc.
Disconnect the Modem from the PC
2
Disconnect the cables that connect your modem to the PC.
Wall Jack
Modem
Exit | Back | Next
Wireless-G ADSL Gateway with SRX200 Setup Wizard Model No. WAG54GX2

**Abbildung 5-4: Setup-Assistent – Fenster *Disconnect the Modem from the PC and ADSL Wall Jack* (Trennen des Modems vom PC und vom ADSL-Splitter)**

6. Der Setup-Assistent fordert Sie auf, das Gateway an den ADSL-Splitter anzuschließen. Klicken Sie anschließend auf die Schaltfläche **Next** (Weiter).

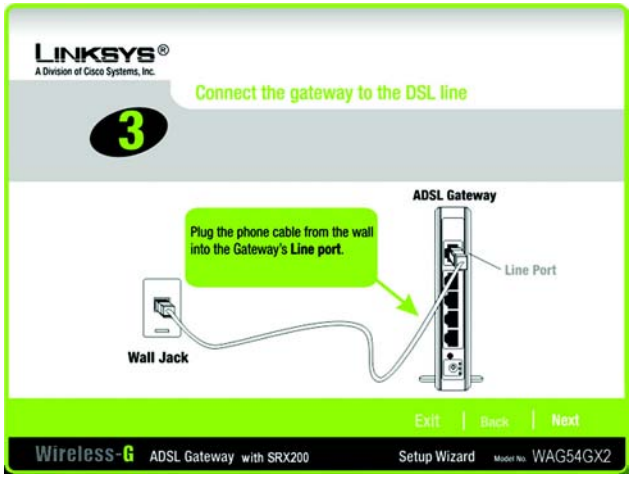
LINKSYS®
A Division of Cisco Systems, Inc.
Connect the gateway to the DSL line
3
ADSL Gateway
Plug the phone cable from the wall into the Gateway's Line port.
Line Port
Wall Jack
Exit | Back | Next
Wireless-G ADSL Gateway with SRX200
Setup Wizard
Model No. WAG54GX2

**Abbildung 5-5: Setup-Assistent – Fenster *Connect the Gateway to the ADSL Wall Jack* (Anschließen des Gateways an den ADSL-Splitter)**

7. Der Setup-Assistent fordert Sie auf, ein Netzwerkkabel an den Computer anzuschließen. Klicken Sie anschließend auf die Schaltfläche **Next** (Weiter).

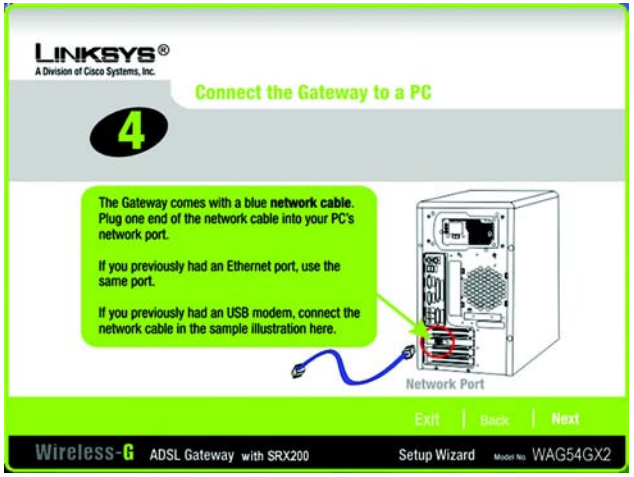
LINKSYS®
A Division of Cisco Systems, Inc.
Connect the Gateway to a PC
4
The Gateway comes with a blue network cable. Plug one end of the network cable into your PC's network port.
If you previously had an Ethernet port, use the same port.
If you previously had an USB modem, connect the network cable in the sample illustration here.
Network Port
Exit | Back | Next
Wireless-G ADSL Gateway with SRX200
Setup Wizard
Model No. WAG54GX2

**Abbildung 5-6: Setup-Assistent – Fenster *Connect a Network Cable to a PC* (Anschließen des Netzwerkkabels an einen PC)**

8. Der Setup-Assistent fordert Sie auf, das andere Ende des Netzwerkkabels an das Gateway anzuschließen.

   Sie können dann weitere Computer an das Gateway anschließen.

   Klicken Sie anschließend auf die Schaltfläche **Next** (Weiter).

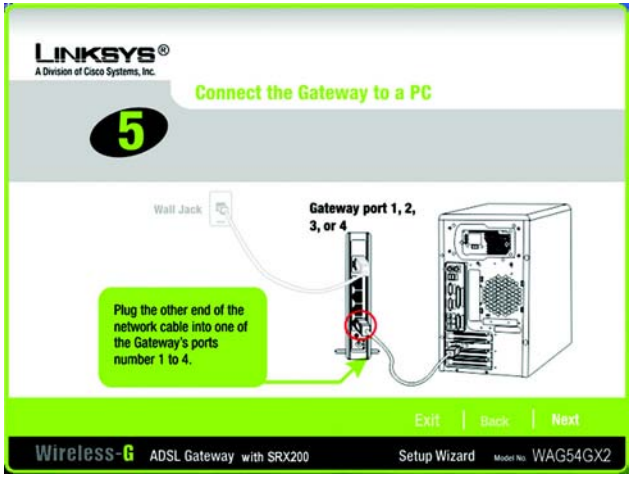
LINKSYS®
A Division of Cisco Systems, Inc.
Connect the Gateway to a PC
5
Wall Jack
Gateway port 1, 2, 3, or 4
Plug the other end of the network cable into one of the Gateway's ports number 1 to 4.
Exit
Back
Next
Wireless-G ADSL Gateway with SRX200
Setup Wizard
Model No. WAG54GX2

**Abbildung 5-7: Setup-Assistent – Fenster *Connect the Network Cable to the Gateway* (Anschließen des Netzwerkkabels an das Gateway)**

9. Der Setup-Assistent fordert Sie auf, das Gateway einzuschalten. Klicken Sie anschließend auf die Schaltfläche **Next** (Weiter).

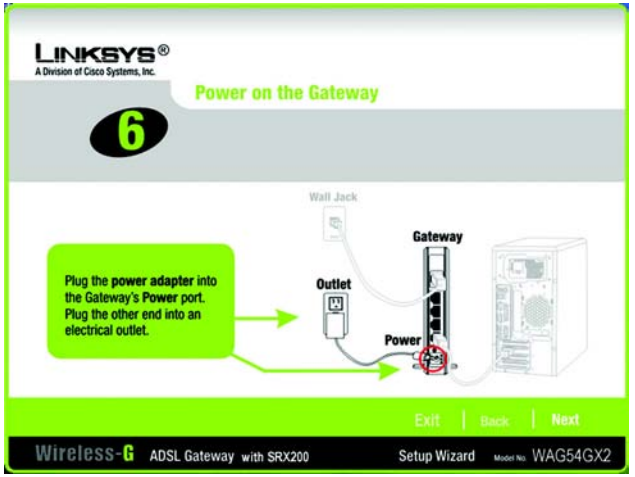


**Abbildung 5-8: Setup-Assistent – Fenster *Power on the Gateway* (Einschalten des Gateways)**

10. Vergewissern Sie sich, dass die LEDs für Netzstrom und DSL sowie die nummerierten LEDs (entsprechend der Anzahl der angeschlossenen Computer) an der Vorderseite des Gateways leuchten. Klicken Sie anschließend auf die Schaltfläche **Next** (Weiter).

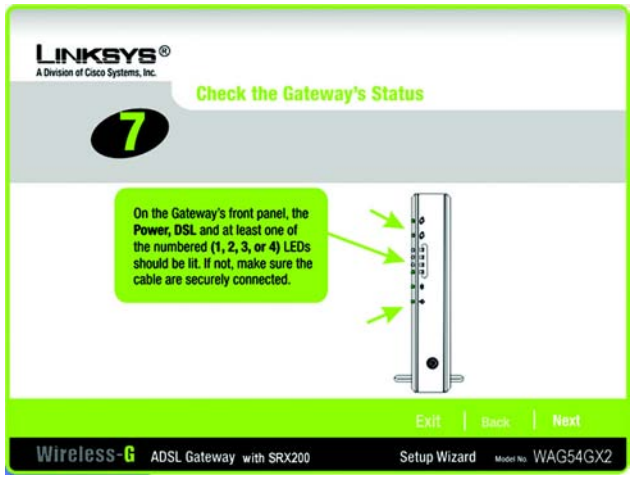
LINKSYS®
A Division of Cisco Systems, Inc.
Check the Gateway's Status
7
On the Gateway's front panel, the Power, DSL and at least one of the numbered (1, 2, 3, or 4) LEDs should be lit. If not, make sure the cable are securely connected.
Exit
Back
Next
Wireless-G ADSL Gateway with SRX200
Setup Wizard
Model No. WAG54GX2

**Abbildung 5-9: Setup-Assistent – Fenster *Check the Gateway's Status* (Überprüfen des Gateway-Status)**

11. Sie werden nach Ihrem Wohnort gefragt. Wählen Sie im Dropdown-Menü das entsprechende Land aus. Klicken Sie anschließend auf die Schaltfläche **Next** (Weiter).

**HINWEIS:** Wenn Ihr Land nicht aufgeführt ist, verwenden Sie zum Konfigurieren der Einstellungen das webbasierte Dienstprogramm des Gateways. Entsprechende Anweisungen finden Sie in „Kapitel 6: Konfigurieren des Wireless-G ADSL-Gateways mit SRX200“.

**Abbildung 5-10: Setup-Assistent – Fenster *Select Your Country* (Auswahl des Landes)**

12. Die Internet-Dienstanbieter (*Internet Service Provider*, ISP) für das ausgewählte Land werden angezeigt. (Je nach dem im vorherigen Fenster ausgewählten Land werden andere Optionen angezeigt.) Klicken Sie auf die Schaltfläche für Ihren ISP.

    Wenn Ihr ISP nicht aufgeführt ist, klicken Sie auf die Schaltfläche **Next** (Weiter), um die Einstellungen manuell einzugeben.

13. Gegebenenfalls erkennt der Setup-Assistent automatisch die verwendete Kapselungsmethode: **1483 Bridged** (1483-Überbrückung), **1483 Routed** (1483-Weiterleitung), **PPPoA** oder **PPPoE**. Wenn Sie die Einstellungen manuell eingeben, wählen Sie zuerst die Kapselungsmethode aus: **1483 Bridged** (1483-Überbrückung), **1483 Routed** (1483-Weiterleitung), **PPPoA** oder **PPPoE**.

    **HINWEIS:** Wenn als Kapselungsmethode **IPoA** oder **Bridge Mode Only** (Nur Überbrückungsmodus) eingesetzt wird, müssen Sie zum Konfigurieren des Gateways das zugehörige webbasierte Dienstprogramm verwenden. Entsprechende Anweisungen finden Sie in „Kapitel 6: Konfigurieren des Wireless-G ADSL-Gateways mit SRX200“.

    Fahren Sie dann mit dem entsprechenden Abschnitt für die ausgewählte Kapselungsmethode fort.

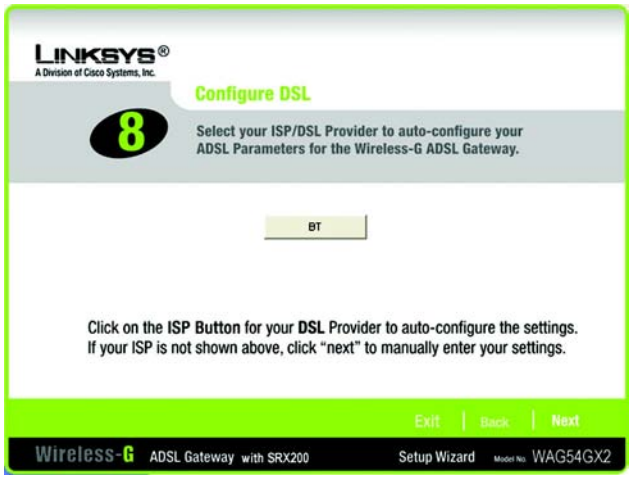
LINKSYS®
A Division of Cisco Systems, Inc.
Configure DSL
8
Select your ISP/DSL Provider to auto-configure your ADSL Parameters for the Wireless-G ADSL Gateway.
BT
Click on the ISP Button for your DSL Provider to auto-configure the settings.
If your ISP is not shown above, click “next” to manually enter your settings.
Exit
Back
Next
Wireless-G ADSL Gateway with SRX200
Setup Wizard
Model No. WAG54GX2

**Abbildung 5-11: Setup-Assistent – Fenster *Select Your Internet Service Provider (UK)* (Auswahl des Internet-Dienstanbieters in Großbritannien)**

## 1483 Bridged (1483-Überbrückung)

Nach der Auswahl eines Internet-Dienstanbieters werden die Einstellungen für Kapselung, VPI, VCI und Multiplexing im Setup-Assistenten automatisch vorgenommen. Wählen Sie dann die entsprechende IP-Einstellung für die DSL-Verbindung aus.

In diesem Fenster können Sie die Einstellungen manuell vornehmen.

**VPI/VCI**: Wenn Sie die Einstellungen manuell eingeben müssen, tragen Sie hier die von Ihrem Internet-Dienstanbieter zur Verfügung gestellten Werte für VPI (*Virtual Path Identifier*) und VCI (*Virtual Channel Identifier*) ein.

**Multiplexing**: Wenn Sie die Einstellungen manuell eingeben müssen, wählen Sie je nach ISP **LLC** oder **VC** aus.

**Auto IP** (Automatische IP-Adresse): Klicken Sie bei Verwendung einer dynamischen IP-Adresse auf das Optionsfeld **Auto IP** (Automatische IP-Adresse).

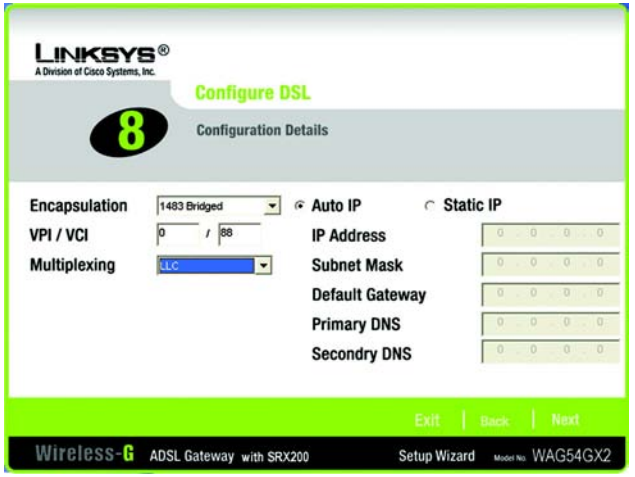


**Abbildung 5-12: Setup-Assistent – Fenster *Configure DSL* (Konfigurieren von DSL) – „1483 Bridged“ (1483-Überbrückung)**

**Static IP** (Statische IP-Adresse): Klicken Sie bei Verwendung einer statischen IP-Adresse auf das Optionsfeld **Static IP** (Statische IP-Adresse). Geben Sie geeignete Werte in den Feldern *IP Address* (IP-Adresse), *Subnet Mask* (Subnetzmaske), *Default Gateway* (Standard-Gateway), *Primary DNS* (Primärer DNS) und *Secondary DNS* (Sekundärer DNS) ein. (Sie müssen mindestens die IP-Adresse eines DNS-Servers eingeben.)

Klicken Sie auf die Schaltfläche **Next** (Weiter), um fortzufahren, oder auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

## 1483 Routed (1483-Weiterleitung)

Nach der Auswahl eines Internet-Dienstanbieters werden die Einstellungen für Kapselung, VPI, VCI und Multiplexing im Setup-Assistenten automatisch vorgenommen. Wählen Sie dann die entsprechenden IP-Einstellungen für die DSL-Verbindung aus.

In diesem Fenster können Sie die Einstellungen manuell vornehmen.

**VPI/VCI**: Wenn Sie die Einstellungen manuell eingeben müssen, tragen Sie hier die von Ihrem Internet-Dienstanbieter zur Verfügung gestellten Werte für VPI (*Virtual Path Identifier*) und VCI (*Virtual Channel Identifier*) ein.

**Multiplexing**: Wenn Sie die Einstellungen manuell eingeben müssen, wählen Sie je nach ISP **LLC** oder **VC** aus.

**Static IP** (Statische IP-Adresse): Geben Sie geeignete Werte in den Feldern *IP Address* (IP-Adresse), *Subnet Mask* (Subnetzmaske), *Default Gateway* (Standard-Gateway), *Primary DNS* (Primärer DNS) und *Secondary DNS* (Sekundärer DNS) ein. (Sie müssen mindestens die IP-Adresse eines DNS-Servers eingeben.)

Klicken Sie auf die Schaltfläche **Next** (Weiter), um fortzufahren, oder auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

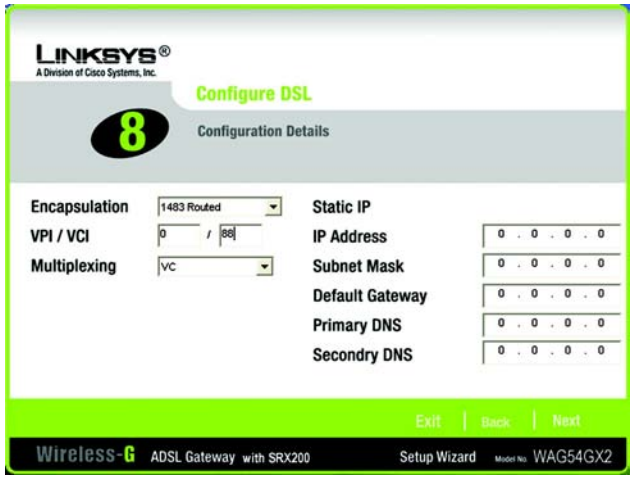


**Abbildung 5-13: Setup-Assistent – Fenster *Configure DSL* (Konfigurieren von DSL) – „1483 Routed“ (1483-Weiterleitung)**

## PPPoA

Nach der Auswahl eines Internet-Dienstanbieters werden die Einstellungen für Kapselung, VPI, VCI und Multiplexing im Setup-Assistenten automatisch vorgenommen. Geben Sie dann die Benutzer-ID und das Passwort für die DSL-Verbindung ein.

In diesem Fenster können Sie die Einstellungen manuell vornehmen.

**VPI/VCI**: Wenn Sie die Einstellungen manuell eingeben müssen, tragen Sie hier die von Ihrem Internet-Dienstanbieter zur Verfügung gestellten Werte für VPI (*Virtual Path Identifier*) und VCI (*Virtual Channel Identifier*) ein.

**Multiplexing**: Wenn Sie die Einstellungen manuell eingeben müssen, wählen Sie je nach ISP **LLC** oder **VC** aus.

**User ID** (Benutzer-ID) und **Password** (Passwort): Geben Sie die Werte für Benutzer-ID und Passwort ein, die Sie von Ihrem ISP erhalten haben.

**Connection** (Verbindung): Wählen Sie für eine ständige Verbindung zu Ihrem ISP die Option **Keep Alive** (Verbindung aufrecht halten), oder wählen Sie **Connect on Demand** (Bei Bedarf verbinden), falls die Verbindungszeit mit Ihrem ISP gebührenpflichtig ist.

**Keep Alive** (Verbindung aufrechterhalten): Bei dieser Option behält der Gateway die Internetverbindung bei. Legen Sie im Feld *Redial Period* (Wahlwiederholung) fest, wie oft die Internetverbindung vom Gateway überprüft werden soll. Die Standardeinstellung beträgt **5** Minuten.

**Connect on Demand** (Bei Bedarf verbinden): Wenn Sie diese Option auswählen, trennt das Gateway die Internetverbindung, nachdem alle Online-Anwendungen in einem angegebenen Zeitraum beendet sind. Dieser Zeitraum wird im Feld *Max Idle Time* (Max. Leerlaufzeit) festgelegt; die Standardeinstellung beträgt **30** Sekunden.

Klicken Sie auf die Schaltfläche **Next** (Weiter), um fortzufahren, oder auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

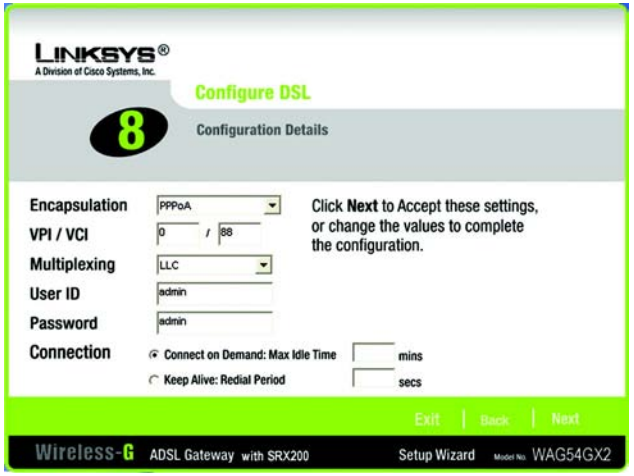


**Abbildung 5-14: Setup-Assistent – Fenster *Configure DSL* (Konfigurieren von DSL) – „PPPoA“**

## PPPoE

Nach der Auswahl eines Internet-Dienstanbieters werden die Einstellungen für Kapselung, VPI, VCI und Multiplexing im Setup-Assistenten automatisch vorgenommen. Geben Sie dann die Benutzer-ID und das Passwort für die DSL-Verbindung ein.

In diesem Fenster können Sie die Einstellungen manuell vornehmen.

**VPI/VCI**: Wenn Sie die Einstellungen manuell eingeben müssen, tragen Sie hier die von Ihrem Internet-Dienstanbieter zur Verfügung gestellten Werte für VPI (*Virtual Path Identifier*) und VCI (*Virtual Channel Identifier*) ein.

**Multiplexing**: Wenn Sie die Einstellungen manuell eingeben müssen, wählen Sie je nach ISP **LLC** oder **VC** aus.

**User ID** (Benutzer-ID) und **Password** (Passwort): Geben Sie die Werte für Benutzer-ID und Passwort ein, die Sie von Ihrem ISP erhalten haben.

**Connection** (Verbindung): Wählen Sie für eine ständige Verbindung zu Ihrem ISP die Option **Keep Alive** (Verbindung aufrecht halten), oder wählen Sie **Connect on Demand** (Bei Bedarf verbinden), falls die Verbindungszeit mit Ihrem ISP gebührenpflichtig ist.

**Keep Alive** (Verbindung aufrechterhalten): Bei dieser Option behält der Gateway die Internetverbindung bei. Legen Sie im Feld *Redial Period* (Wahlwiederholung) fest, wie oft die Internetverbindung vom Gateway überprüft werden soll. Die Standardeinstellung beträgt **5** Minuten.

**Connect on Demand** (Bei Bedarf verbinden): Wenn Sie diese Option auswählen, trennt das Gateway die Internetverbindung, nachdem alle Online-Anwendungen in einem angegebenen Zeitraum beendet sind. Dieser Zeitraum wird im Feld *Max Idle Time* (Max. Leerlaufzeit) festgelegt; die Standardeinstellung beträgt **30** Sekunden.

Klicken Sie auf die Schaltfläche **Next** (Weiter), um fortzufahren, oder auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

14. Für das Gateway steht ein webbasiertes Dienstprogramm zur Verfügung, mit dem Sie das Gateway über jeden Netzwerkcomputer konfigurieren können. Der Zugriff auf das Dienstprogramm ist passwortgeschützt.

    **Password** (Passwort): Das Standardpasswort lautet **admin**. Ändern Sie es in ein Passwort Ihrer Wahl.

    **Confirm** (Bestätigen): Geben Sie im Feld *Confirm* (Bestätigen) das Passwort erneut ein.

    Klicken Sie auf die Schaltfläche **Next** (Weiter), um fortzufahren, oder auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

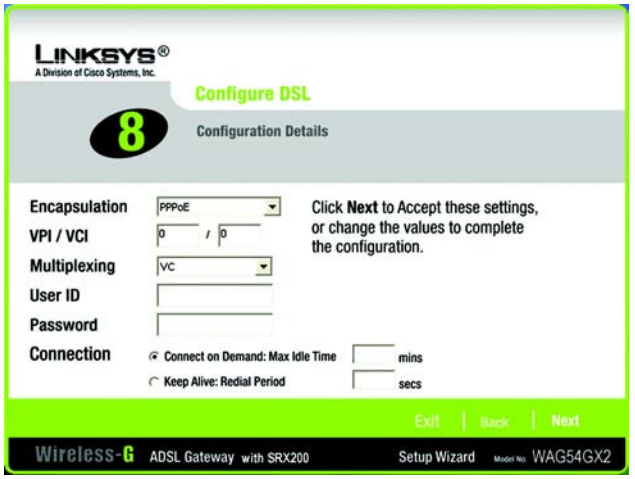


**Abbildung 5-15: Setup-Assistent – Fenster *Configure DSL* (Konfigurieren von DSL) – „PPPoE“**

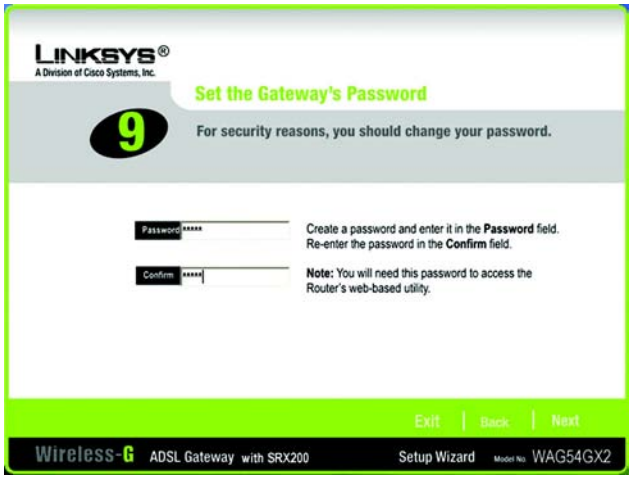


**Abbildung 5-16: Setup-Assistent – Fenster *Set the Gateway's Password* (Einrichten des Gateway-Passworts)**

15. Der Setup-Assistent fordert Sie auf, die Einstellungen für das Wireless-Netzwerk einzugeben.

**SSID**: Geben Sie im Feld *SSID* den Namen des Wireless-Netzwerks ein. Die SSID muss für alle Geräte im Netzwerk identisch sein. Die Standardeinstellung ist **linksys** (Kleinbuchstaben).

**HINWEIS:** Bei der SSID handelt es sich um den Netzwerknamen, der von allen Geräten in einem Wireless-Netzwerk gemeinsam verwendet wird. Die SSID Ihres Netzwerks muss eindeutig und für alle Geräte im Netzwerk identisch sein.

**Channel** (Kanal): Wählen Sie den Betriebskanal für Ihr Wireless-Netzwerk aus. Über diesen Kanal kommunizieren alle Wireless-Geräte.

**Network Mode** (Netzwerkmodus): Wählen Sie im Dropdown-Menü *Network Mode* (Netzwerkmodus) die Wireless-Standards aus, die im Netzwerk verwendet werden. Wenn sich sowohl 802.11g- als auch 802.11b-Geräte in Ihrem Netzwerk befinden, behalten Sie die Standardeinstellung **Mixed** (Gemischt) bei. Wenn ausschließlich 802.11g-Geräte vorhanden sind, wählen Sie **G-Only** (Nur G) aus. Wenn ausschließlich 802.11b-Geräte vorhanden sind, wählen Sie **B-Only** (Nur B) aus. Wenn Sie das Wireless-Netzwerk deaktivieren möchten, wählen Sie **Disable** (Deaktivieren) aus.

**Device Name** (Gerätename): Geben Sie im Feld *Device Name* (Gerätename) einen Namen für das Gateway ein.

Klicken Sie auf die Schaltfläche **Next** (Weiter), um fortzufahren, oder auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

16. Wählen Sie die zu verwendende Sicherheitsmethode aus: **WPA Personal**, **WPA2 Personal**, **WPA2 Mixed Mode** (WPA2 Gemischter Modus), **WEP (64-Bit)** oder **WEP (128-Bit)**. WPA ist die Abkürzung für *Wi-Fi Protected Access*, WEP für *Wired Equivalent Privacy*. WPA bietet eine höhere Sicherheit als WEP. Bei WPA2 handelt es sich um eine WPA-Version mit stärkerer Verschlüsselung. Fahren Sie mit den entsprechenden Anweisungen für die gewünschte Sicherheitsmethode fort.

Wenn Sie keine Wireless-Sicherheitsmethode verwenden möchten, klicken Sie auf **Disabled** (Deaktiviert) und dann auf die Schaltfläche **Next** (Weiter). Fahren Sie mit Schritt 17 fort.

**HINWEIS:** Wenn Sie die Sicherheitsmethode WPA Enterprise oder WPA2 Enterprise verwenden möchten, klicken Sie auf **Disabled** (Deaktiviert) und dann auf die Schaltfläche **Next** (Weiter). Sobald Sie den Setup-Assistenten beendet haben, konfigurieren Sie die Wireless-Sicherheitseinstellungen mit dem webbasierten Dienstprogramm des Gateways. Entsprechende Anweisungen finden Sie in „Kapitel 6: Konfigurieren des Wireless-G ADSL-Gateways mit SRX200“.

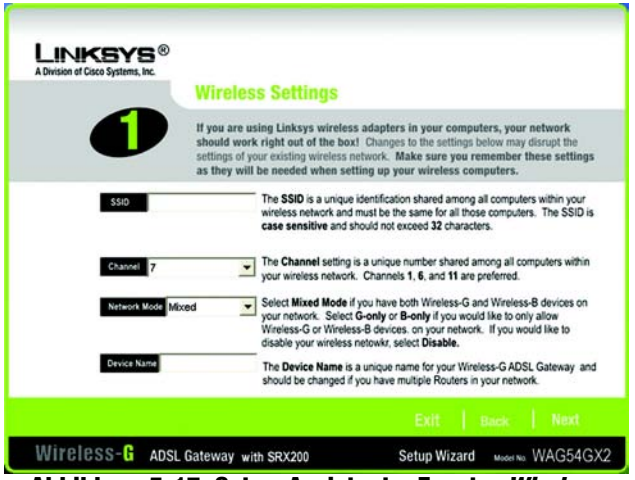
LINKSYS®
A Division of Cisco Systems, Inc.
Wireless Settings
1
If you are using Linksys wireless adapters in your computers, your network should work right out of the box! Changes to the settings below may disrupt the settings of your existing wireless network. Make sure you remember these settings as they will be needed when setting up your wireless computers.
SSID
The SSID is a unique identification shared among all computers within your wireless network and must be the same for all those computers. The SSID is case sensitive and should not exceed 32 characters.
Channel 7
The Channel setting is a unique number shared among all computers within your wireless network. Channels 1, 6, and 11 are preferred.
Network Mode Mixed
Select Mixed Mode if you have both Wireless-G and Wireless-B devices on your network. Select G-only or B-only if you would like to only allow Wireless-G or Wireless-B devices. on your network. If you would like to disable your wireless netowkr, select Disable.
Device Name
The Device Name is a unique name for your Wireless-G ADSL Gateway and should be changed if you have multiple Routers in your network.
Exit | Back | Next
Wireless-G ADSL Gateway with SRX200
Setup Wizard Model No. WAG54GX2

**Abbildung 5-17: Setup-Assistent – Fenster *Wireless Settings* (Wireless-Einstellungen)**

***WPA** (Wi-Fi Protected Access): Ein Wireless-Sicherheitsprotokoll, bei dem eine TKIP-Verschlüsselung (Temporal Key Integrity Protocol) verwendet wird, die zusammen mit einem RADIUS-Server eingesetzt werden kann.*

***WEP** (Wired Equivalent Privacy): Eine hochgradig sichere Methode zum Verschlüsseln von Netzwerkdaten, die in einem Wireless-Netzwerk übertragen werden.*

LINKSYS®
A Division of Cisco Systems, Inc.
Configure Wireless Security Settings (Optional)
2
Security
You may choose between five encryption methods: 64-Bit Wired-Equivalent Privacy (WEP), 128-Bit WEP, WPA Personal (Pre-shared key), WPA2 Personal or WPA2 Mixed Mode. The security settings must be the same on all devices on your network, or they will not be able to communicate.
Security Disable
Please choose WEP (64-Bit), WEP (128-Bit), WPA Personal, WPA2 Personal, WPA2 Mixed Mode or Disabled.
Disable
WEP (64-bit)
WEP (128-bit)
WPA Personal
WPA2 Personal
WPA2 Mixed Mode
Exit | Back | Next
Wireless-G ADSL Gateway with SRX200
Setup Wizard Model No. WAG54GX2

**Abbildung 5-18: Setup-Assistent – Fenster *Configure Wireless Security Settings* (Konfigurieren der Wireless-Sicherheitseinstellungen)**

## WPA Personal

**Encryption** (Verschlüsselung): Wählen Sie den gewünschten Algorithmus aus (**TKIP** oder **AES**).

**Passphrase**: Geben Sie eine Passphrase (auch als vorläufiger gemeinsamer Schlüssel bezeichnet) mit einer Länge von 8 bis 63 Zeichen ein. Je länger und komplexer Ihre Passphrase ist, desto sicherer ist Ihr Netzwerk.

Klicken Sie auf die Schaltfläche **Next** (Weiter), um fortzufahren, oder auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

***Verschlüsselung**: Die Codierung von Daten, die über ein Netzwerk übertragen werden.*

LINKSYS®
A Division of Cisco Systems, Inc.
Configure Wireless Security Settings (Optional)
2
Security
You may choose between five encryption methods: 64-Bit Wired-Equivalent Privacy (WEP), 128-Bit WEP, WPA Personal (Pre-shared key), WPA2 Personal or WPA2 Mixed Mode. The security settings must be the same on all devices on your network, or they will not be able to communicate.
Security
WPA Personal
Please choose WEP (64-Bit), WEP (128-Bit), WPA Personal, WPA2 Personal, WPA2 Mixed Mode or Disabled.
Encryption
TKIP
TKIP
AES
Select the type of Encryption your Network uses.
Passphrase
Enter the Passphrase key used by your network. The Passphrase Key can be any keyboard character between 8 and 63 characters in length.
Exit | Back | Next
Wireless-G ADSL Gateway with SRX200
Setup Wizard
Model No. WAG54GX2

**Abbildung 5-19: Setup-Assistent – Fenster *Wireless Security* (Wireless-Sicherheit) – „WPA Personal“**

## WPA2 Personal

**Encryption** (Verschlüsselung): Für den Modus **WPA2 Personal** wird automatisch die Option **AES** ausgewählt.

**Passphrase**: Geben Sie eine Passphrase (auch als vorläufiger gemeinsamer Schlüssel bezeichnet) mit einer Länge von 8 bis 63 Zeichen ein. Je länger und komplexer Ihre Passphrase ist, desto sicherer ist Ihr Netzwerk.

Klicken Sie auf die Schaltfläche **Next** (Weiter), um fortzufahren, oder auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

LINKSYS®
A Division of Cisco Systems, Inc.
Configure Wireless Security Settings (Optional)
2
Security
You may choose between five encryption methods: 64-Bit Wired-Equivalent Privacy (WEP), 128-Bit WEP, WPA Personal (Pre-shared key), WPA2 Personal or WPA2 Mixed Mode. The security settings must be the same on all devices on your network, or they will not be able to communicate.
Security
WPA2 Personal
Please choose WEP (64-Bit), WEP (128-Bit), WPA Personal, WPA2 Personal, WPA2 Mixed Mode or Disabled.
Encryption
AES
AES
Select the type of Encryption your Network uses.
Passphrase
Enter the Passphrase key used by your network. The Passphrase Key can be any keyboard character between 8 and 63 characters in length.
Exit | Back | Next
Wireless-G ADSL Gateway with SRX200
Setup Wizard
Model No. WAG54GX2

**Abbildung 5-20: Setup-Assistent – Fenster *Wireless Security* (Wireless-Sicherheit) – „WPA2 Personal“**

## WPA2 Mixed Mode (WPA2 Gemischter Modus)

**Encryption** (Verschlüsselung): Es wird automatisch **TKIP + AES** ausgewählt, so dass beide Methoden verwendet werden können.

**Passphrase**: Geben Sie eine Passphrase (auch als vorläufiger gemeinsamer Schlüssel bezeichnet) mit einer Länge von 8 bis 63 Zeichen ein. Je länger und komplexer Ihre Passphrase ist, desto sicherer ist Ihr Netzwerk.

Klicken Sie auf die Schaltfläche **Next** (Weiter), um fortzufahren, oder auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

LINKSYS®
A Division of Cisco Systems, Inc.
Configure Wireless Security Settings (Optional)
2
Security
You may choose between five encryption methods: 64-Bit Wired-Equivalent Privacy (WEP), 128-Bit WEP, WPA Personal (Pre-shared key), WPA2 Personal or WPA2 Mixed Mode. The security settings must be the same on all devices on your network, or they will not be able to communicate.
Security
WPA2 Mixed Mode
Please choose WEP (64-Bit), WEP (128-Bit), WPA Personal, WPA2 Personal, WPA2 Mixed Mode or Disabled.
Encryption
TKIP + AES
TKIP + AES
Select the type of Encryption your Network uses.
Passphrase
Enter the Passphrase key used by your network. The Passphrase Key can be any keyboard character between 8 and 63 characters in length.
Exit
Back
Next
Wireless-G ADSL Gateway with SRX200
Setup Wizard
Model No. WAG54GX2

**Abbildung 5-21: Setup-Assistent – Fenster *Wireless Security* (Wireless-Sicherheit) – „WPA2 Mixed Mode“ (WPA2 Gemischter Modus)**

## WEP (64-Bit)

Geben Sie eine Passphrase oder einen WEP-Schlüssel ein.

**Passphrase**: Geben Sie eine Passphrase in das Feld *Passphrase* ein, sodass automatisch ein WEP-Schlüssel generiert wird. Bei der Passphrase wird zwischen Groß- und Kleinschreibung unterschieden. Die Länge von 16 alphanumerischen Zeichen darf nicht überschritten werden. Sie muss mit den Passphrasen Ihrer anderen Wireless-Netzwerkgeräte übereinstimmen und ist nur mit Wireless-Produkten von Linksys kompatibel. (Wenn Sie Wireless-Produkte anderer Anbieter verwenden, geben Sie den WEP-Schlüssel bei den entsprechenden Produkten manuell ein.)

**Key 1** (Schlüssel 1): Der eingegebene WEP-Schlüssel muss mit dem WEP-Schlüssel des Wireless-Netzwerks übereinstimmen. Geben Sie für die 64-Bit-Verschlüsselung genau 10 hexadezimale Zeichen ein. Gültige hexadezimale Zeichen sind Zeichen von „0“ bis „9“ und von „A“ bis „F“.

Klicken Sie auf die Schaltfläche **Next** (Weiter), um fortzufahren, oder auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

LINKSYS®
A Division of Cisco Systems, Inc.
Configure Wireless Security Settings (Optional)
2
Security
You may choose between five encryption methods: 64-Bit Wired-Equivalent Privacy (WEP), 128-Bit WEP, WPA Personal (Pre-shared key), WPA2 Personal or WPA2 Mixed Mode. The security settings must be the same on all devices on your network, or they will not be able to communicate.
Security
WEP (64-bit)
Please choose WEP (64-Bit), WEP (128-Bit), WPA Personal, WPA2 Personal, WPA2 Mixed Mode or Disabled.
Passphrase
Type the passphrase that will be used to generate the WEP key. The passphrase is case-sensitive and should not be longer than 16 characters.
Key 1
If you choose the Passphrase option for WEP, a WEP key will generate automatically. To manually enter a WEP key, select a WEP algorithm and leave the Passphrase option blank
Exit
Back
Next
Wireless-G ADSL Gateway with SRX200
Setup Wizard
Model No. WAG54GX2

**Abbildung 5-22: Setup-Assistent – Fenster *Wireless Security* (Wireless-Sicherheit) – „WEP (64-Bit)“**

### WEP (128-Bit)

Geben Sie eine Passphrase oder einen WEP-Schlüssel ein.

**Passphrase**: Geben Sie eine Passphrase in das Feld *Passphrase* ein, sodass automatisch ein WEP-Schlüssel generiert wird. Bei der Passphrase wird zwischen Groß- und Kleinschreibung unterschieden. Die Länge von 16 alphanumerischen Zeichen darf nicht überschritten werden. Sie muss mit den Passphrasen Ihrer anderen Wireless-Netzwerkgeräte übereinstimmen und ist nur mit Wireless-Produkten von Linksys kompatibel. (Wenn Sie Wireless-Produkte anderer Anbieter verwenden, geben Sie den WEP-Schlüssel bei den entsprechenden Produkten manuell ein.)

**Key 1** (Schlüssel 1): Der eingegebene WEP-Schlüssel muss mit dem WEP-Schlüssel des Wireless-Netzwerks übereinstimmen. Geben Sie für die 128-Bit-Verschlüsselung genau 26 hexadezimale Zeichen ein. Gültige hexadezimale Zeichen sind Zeichen von „0“ bis „9“ und von „A“ bis „F“.

Klicken Sie auf die Schaltfläche **Next** (Weiter), um fortzufahren, oder auf die Schaltfläche **Back** (Zurück), um zum vorherigen Fenster zurückzukehren.

LINKSYS®
A Division of Cisco Systems, Inc.
Configure Wireless Security Settings (Optional)
2
Security
You may choose between five encryption methods: 64-Bit Wired-Equivalent Privacy (WEP), 128-Bit WEP, WPA Personal (Pre-shared key), WPA2 Personal or WPA2 Mixed Mode. The security settings must be the same on all devices on your network, or they will not be able to communicate.
Security
WEP (128-bit)
Please choose WEP (64-Bit), WEP (128-Bit), WPA Personal, WPA2 Personal, WPA2 Mixed Mode or Disabled.
Passphrase
Type the passphrase that will be used to generate the WEP key. The passphrase is case-sensitive and should not be longer than 16 characters.
Key 1
If you choose the Passphrase option for WEP, a WEP key will generate automatically. To manually enter a WEP key, select a WEP algorithm and leave the Passphrase option blank
Exit
Back
Next
Wireless-G ADSL Gateway with SRX200
Setup Wizard
Model No. WAG54GX2

**Abbildung 5-23: Setup-Assistent – Fenster *Wireless Security* (Wireless-Sicherheit) – „WEP (128-Bit)“**

17. Der Setup-Assistent fordert Sie auf, die Einstellungen vor dem Speichern zu überprüfen. Wenn Sie mit den Einstellungen zufrieden sind, klicken Sie auf die Schaltfläche **Yes** (Ja). Klicken Sie auf die Schaltfläche **No** (Nein), falls Sie die neuen Einstellungen nicht speichern möchten.

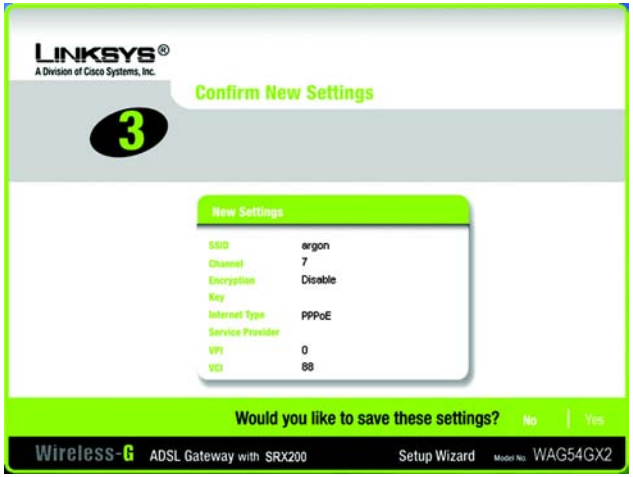


**Abbildung 5-24: Setup-Assistent – Fenster *Confirm New Settings* (Bestätigen der neuen Einstellungen)**

18. Nach dem Speichern der Einstellungen wird das Fenster *Safe Surfing* (Sicheres Surfen) angezeigt. Klicken Sie auf die Schaltfläche **Norton Internet Security Suite**, um Norton Internet Security Special Edition auf dem Computer zu installieren, oder auf die Schaltfläche **Finish** (Fertig stellen), um den Setup-Assistenten zu beenden.

LINKSYS
A Division of Cisco Systems, Inc.
Norton Internet Security™ from Symantec™ is the award winning suite which protects your PCs and your family from the perils of the Internet.
- Norton AntiVirus™ protects email and instant messages.
- Norton™ Personal Firewall protects against hackers and intrusions.
- Parental Control shields children from objectionable web sites.
- Blocks spam, banner ads, pop-up windows, and more.
A special edition of Norton Internet Security with a 60-day free trial of virus & firewall updates is included on this Setup CD.
Click below to install it.
symantec.
Internet Security
Special Edition
Includes 60-day free trial of virus & firewall updates
Norton Internet Security Suite
Safe Surfing
Setup Wizard
Finish
Cisco Systems
© Copyright 2005 Cisco Systems, Inc. All rights reserved.

**Abbildung 5-25: Setup-Assistent – Fenster *Safe Surfing* (Sicheres Surfen)**

19. Das Fenster *Congratulations* (Herzlichen Glückwunsch) wird angezeigt. Klicken Sie auf die Schaltfläche **Online Registration** (Online-Registrierung), um das Gateway zu registrieren, oder auf die Schaltfläche **Exit** (Beenden), um den Setup-Assistenten zu beenden.

**Herzlichen Glückwunsch! Die Installation des Wireless-G ADSL-Gateways mit SRX200 ist hiermit abgeschlossen.**

**Wenn Sie komplexere Änderungen an der Konfiguration vornehmen möchten, fahren Sie mit „Kapitel 6: Konfigurieren des Wireless-G ADSL-Gateways mit SRX200“ fort.**

**Abbildung 5-26: Setup-Assistent – Fenster *Congratulations* (Herzlichen Glückwunsch)**

# Kapitel 6: Konfigurieren des Wireless-G ADSL-Gateways mit SRX200

## Übersicht

Konfigurieren Sie das Gateway anhand der Anweisungen in diesem Kapitel und mithilfe des webbasierten Dienstprogramms des Gateways. In diesem Kapitel werden alle Webseiten des Dienstprogramms und deren Hauptfunktionen beschrieben. Sie können das Dienstprogramm über einen an das Gateway angeschlossenen Computer mit dem Webbrowser aufrufen. Bei der grundlegenden Netzwerkeinrichtung verwenden die meisten Benutzer die folgenden Fenster des Dienstprogramms:

- **Basic Setup** (Grundlegende Einrichtung): Geben Sie im Fenster **Basic Setup** (Grundlegende Einrichtung) die von Ihrem Internet-Dienstanbieter bereitgestellten Einstellungen ein.
- **Management** (Verwaltungsfunktionen): Klicken Sie auf die Registerkarte **Administration** (Verwaltung) und anschließend auf die Registerkarte **Management** (Verwaltungsfunktionen). Der Standardbenutzername und das Standardpasswort des Gateways lauten **admin**. Ändern Sie zum Schutz des Gateways den Standardbenutzernamen und das Passwort.

Es stehen sieben Hauptregisterkarten zur Verfügung: **Setup** (Einrichtung), **Wireless**, **Security** (Sicherheit), **Access Restrictions** (Zugriffsbeschränkungen), **Applications & Gaming** (Anwendungen & Spiele), **Administration** (Verwaltung) und **Status**. Wenn Sie auf eine der Hauptregisterkarten klicken, sind jeweils zusätzliche Registerkarten verfügbar. Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

### Einrichtung

- **Basic Setup** (Grundlegende Einrichtung): Geben Sie in diesem Fenster die Internetverbindung und die Netzwerkeinstellungen ein.
- **DDNS**: Füllen Sie die Felder dieses Fensters aus, um die Funktion **DDNS** (*Dynamic Domain Name System*) des Gateways zu aktivieren.
- **Advanced Routing** (Erweitertes Routing): In diesem Fenster können Sie die Konfigurationseinstellungen für NAT und Routing ändern.

**HABEN SIE:** TCP/IP auf den Computern aktiviert? Computer tauschen mit diesem Protokoll über das Netzwerk Daten aus. Weitere Informationen zu TCP/IP erhalten Sie in der Windows-Hilfe.

**HINWEIS:** Zur zusätzlichen Sicherheit sollten Sie den Benutzernamen und das Passwort auf der Registerkarte **Administration** (Verwaltung) ändern.

## Wireless

- **Basic Wireless Settings** (Grundlegende Wireless-Einstellungen): In diesem Fenster können Sie die Wireless-Netzwerkeinstellungen auswählen.
- **Wireless Security** (Wireless-Sicherheit): Konfigurieren Sie in diesem Fenster die Wireless-Sicherheitseinstellungen.
- **Wireless Access** (Wireless-Zugriff): In diesem Fenster können Sie den Zugriff auf das Wireless-Netzwerk steuern.
- **Advanced Wireless Settings** (Erweiterte Wireless-Einstellungen): Über dieses Fenster können Sie auf die erweiterten Wireless-Netzwerkeinstellungen zugreifen.

## Sicherheit

- **Firewall**: In diesem Fenster können Sie die Firewall aktivieren bzw. deaktivieren, Filter einrichten und anonyme Internet-Anfragen blockieren.
- **VPN Passthrough** (VPN-Passthrough): In diesem Fenster können Sie VPN-Passthrough (*Virtual Private Network*) aktivieren oder deaktivieren.
- **VPN**: In diesem Fenster können Sie bis zu fünf VPN-Tunnel konfigurieren.

***VPN** (Virtual Private Network): Eine Sicherheitsmaßnahme, mit der Daten geschützt werden, wenn sie über das Internet von einem Netzwerk in ein anderes übertragen werden.*

## „Access Restrictions“ (Zugriffsbeschränkungen)

- **Internet Access Policy** (Richtlinien für Internetzugriff): In diesem Fenster können Sie die Internetverwendung und den Datenverkehr im lokalen Netzwerk steuern.

## „Applications & Gaming“ (Anwendungen & Spiele)

- **Single Port Range Forwarding** (Einfache Anschlussweiterleitung): In diesem Fenster können Sie gängige Dienste oder Anwendungen einrichten, für die das Weiterleiten eines einzelnen Ports erforderlich ist.
- **Port Range Forwarding** (Weiterleitung an einen Anschlussbereich): In diesem Fenster können Sie öffentliche Dienste oder andere spezielle Internetanwendungen einrichten, für die das Weiterleiten eines Anschlussbereichs erforderlich ist.
- **Port Range Triggering** (Anschlussbereich-Triggering): Klicken Sie auf diese Registerkarte, um die Bereiche für Port-Triggering und Port-Forwarding für Internetanwendungen festzulegen.

- **DMZ**: Richten Sie in diesem Fenster die Internetverbindung für einen lokalen Computer so ein, dass spezielle Dienste verwendet werden können.
- **QoS**: Ordnen Sie mit QoS (*Quality of Service*) unterschiedliche Arten der Datenübertragung verschiedenen Prioritätsstufen zu.

## „Administration“ (Verwaltungsfunktionen)

- **Management** (Verwaltungsfunktionen): In diesem Fenster können Sie den Gateway-Zugriff sowie die Einstellungen für SNMP (*Simple Network Management Protocol*), UPnP (*Universal Plug and Play*), die Wireless-Verwaltung und die IGMP-Proxy-Einstellungen ändern.
- **Reporting** (Berichtaufzeichnung): Klicken Sie auf diese Registerkarte, um Aktivitätsprotokolle anzuzeigen oder zu speichern.
- **Diagnostics** (Diagnose): In diesem Fenster können Sie Ping-Tests ausführen.
- **Backup & Restore** (Sichern & Wiederherstellen): In diesem Fenster können Sie die Konfiguration des Gateways sichern und wiederherstellen.
- **Factory Defaults** (Werkseinstellungen): In diesem Fenster können Sie die Werkseinstellungen des Gateways wiederherstellen.
- **Firmware Upgrade** (Aktualisieren der Firmware): Klicken Sie auf diese Registerkarte, um die Gateway-Firmware zu aktualisieren.

## Status

- **Gateway**: In diesem Fenster sind die Statusinformationen des Gateways aufgeführt.
- **Local Network** (Lokales Netzwerk): In diesem Fenster sind die Statusinformationen des lokalen Netzwerks aufgeführt.
- **Wireless** (Wireless-Netzwerk): In diesem Fenster sind die Statusinformationen des Wireless-Netzwerks aufgeführt.
- **DSL Connection** (DSL-Verbindung): In diesem Fenster sind die Statusinformationen der DSL-Verbindung aufgeführt.

## Hinweis für den Zugriff auf das webbasierte Dienstprogramm

Wenn Sie auf das webbasierte Dienstprogramm zugreifen möchten, starten Sie Internet Explorer oder Netscape Navigator, und geben Sie im Feld *Adresse* die Standard-IP-Adresse des Gateways (**192.168.1.1**) ein. Drücken Sie anschließend die Eingabetaste.

Daraufhin wird ein Anmeldefenster angezeigt. (Unter Windows XP wird ein ähnliches Fenster angezeigt.) Geben Sie **admin** (Standardbenutzername) im Feld *Benutzername* und **admin** (Standardkennwort) im Feld *Kennwort* ein. Klicken Sie anschließend auf die Schaltfläche **OK**.

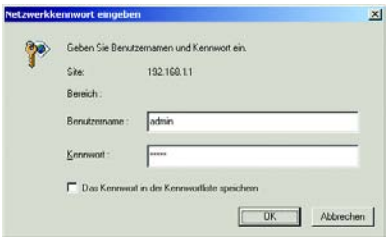


**Abbildung 6-1: Anmeldefenster**

## Registerkarte „Setup“ (Einrichtung)

### Registerkarte „Basic Setup“ (Grundlegende Einrichtung)

Im ersten geöffneten Fenster wird die Registerkarte **Basic Setup** (Grundlegende Einrichtung) angezeigt. Auf dieser Registerkarte können Sie die allgemeinen Einstellungen des Gateways ändern. Ändern Sie die Einstellungen entsprechend den folgenden Erläuterungen, und klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu übernehmen, oder auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen), um die Änderungen zu verwerfen. Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

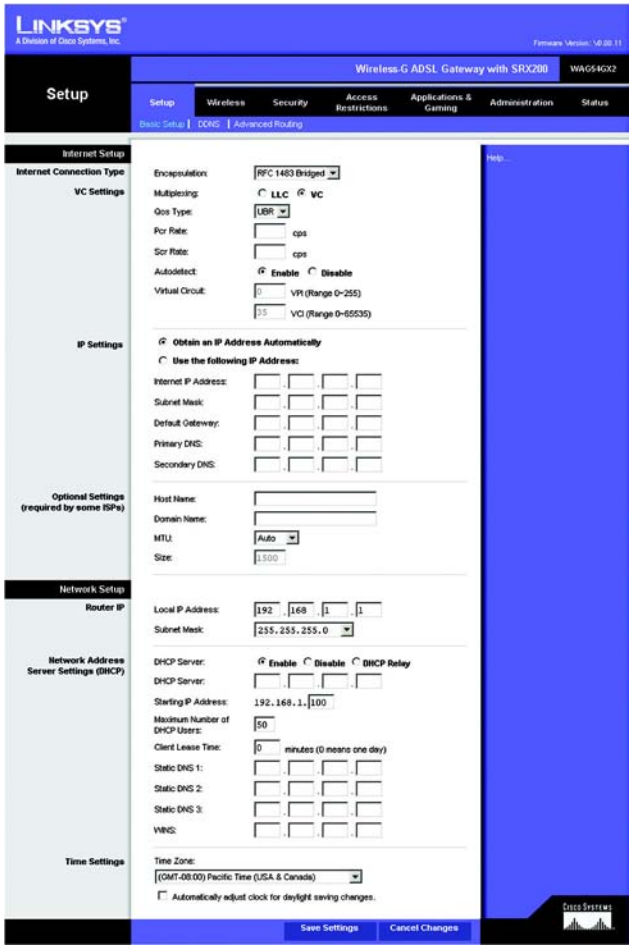


**Abbildung 6-2: „Basic Setup“ (Grundlegende Einrichtung)**

#### „Internet Setup“ (Internet-Einrichtung)

- **Internet Connection Type** (Internet-Verbindungstyp): Das Gateway unterstützt sechs Kapselungstypen: **RFC 1483 Bridged** (RFC 1483-Überbrückung), **RFC 1483 Routed** (RFC 1483-Weiterleitung), **IPoA**, **RFC 2516 PPPoE**, **RFC 2364 PPPoA** und **Bridge Mode Only** (Nur Überbrückungsmodus). Wählen Sie im Dropdown-Menü den gewünschten Kapselungstyp aus. Das jeweilige Fenster *Basic Setup* (Grundlegende Einrichtung) und die verfügbaren Funktionen unterscheiden sich je nach ausgewähltem Kapselungstyp.

- **VC Settings** (VC-Einstellungen): In diesem Bereich können Sie die VC-Einstellungen (*Virtual Circuit*, virtuelle Verbindung) konfigurieren.

  - **Multiplexing**: Wählen Sie entsprechend dem verwendeten ISP die Option **LLC** (LLC-Multiplexing) oder **VC** (VC-Multiplexing) aus.

  - **QoS Type** (QoS-Typ): Wählen Sie im Dropdown-Menü eine der folgenden Optionen aus: **CBR** (*Continuous Bit Rate*, Konstante Bitrate), um eine feste Bandbreite für Sprach- oder Datenverkehr festzulegen, **UBR** (*Unspecific Bit Rate*, Unbestimmte Bitrate) für Anwendungen, die zeitunabhängig sind (z. B. E-Mail), oder **VBR** (*Variable Bit Rate*, Variable Bitrate) für diskontinuierlichen Datenverkehr und Bandbreiten, die mit anderen Anwendungen gemeinsam verwendet werden.

- **Pcr Rate** (PCR-Rate): Wenn Sie die Übertragungsrate der DSL-Leitung durch 424 dividieren, erhalten Sie die PCR-Rate. Diese gibt die maximale Rate an, mit der ein Sender Zellen senden kann. Geben Sie die Rate in diesem Feld ein (sofern dies für den Dienstanbieter erforderlich ist).

- **Scr Rate** (SCR-Rate): Gibt den Mittelwert der Zellrate an, die übertragen werden kann. Der Wert der SCR-Rate liegt gewöhnlich unter dem Wert der PCR-Rate. Geben Sie die Rate in diesem Feld ein (sofern dies für den Dienstanbieter erforderlich ist).

- **Autodetect** (Automatisch erkennen): Wählen Sie **Enable** (Aktivieren) aus, damit die Einstellungen automatisch eingetragen werden, oder **Disable** (Deaktivieren), um die Werte manuell einzugeben.

- **Virtual Circuit** (Virtuelle Verbindung): Für diese Option sind zwei Einstellungen erforderlich: **VPI** (*Virtual Path Identifier*, Virtueller Pfadidentifizierer) und **VCI** (*Virtual Channel Identifier*, Virtueller Kanalidentifizierer). Die korrekten Einstellungen erhalten Sie von Ihrem ISP.

- **IP Settings** (IP-Einstellungen): Befolgen Sie die Anweisungen, die im Abschnitt für den jeweils verwendeten Kapselungstyp aufgeführt sind.

### „RFC 1483 Bridged“ (RFC 1483-Überbrückung)

### Dynamische IP-Adresse

**IP Settings** (IP-Einstellungen): Aktivieren Sie **Obtain an IP Address Automatically** (IP-Adresse automatisch beziehen), wenn Sie laut Angaben Ihres ISP die Verbindung über eine dynamische IP-Adresse herstellen.

### Statische IP-Adresse

Wenn Sie für die Internetverbindung eine permanente (statische) IP-Adresse verwenden, aktivieren Sie **Use the following IP Address** (Folgende IP-Adresse verwenden).

- **Internet IP Address** (Internet-IP-Adresse): Hierbei handelt es sich um die IP-Adresse des Gateways im WAN bzw. im Internet. Sie erhalten die hier anzugebene IP-Adresse von Ihrem ISP.

- **Subnet Mask** (Subnetzmaske): Hierbei handelt es sich um die Subnetzmaske des Gateways. Sie erhalten die Subnetzmaske von Ihrem ISP.

- **Default Gateway** (Standard-Gateway): Sie erhalten die Standard-Gateway-Adresse von Ihrem ISP. Bei dieser Adresse handelt es sich um die IP-Adresse des ISP-Servers.

- **Primary DNS** (Primärer DNS, erforderlich) und **Secondary DNS** (Sekundärer DNS, optional): Sie erhalten von Ihrem ISP mindestens eine Server-IP-Adresse für das DNS (*Domain Name System*).

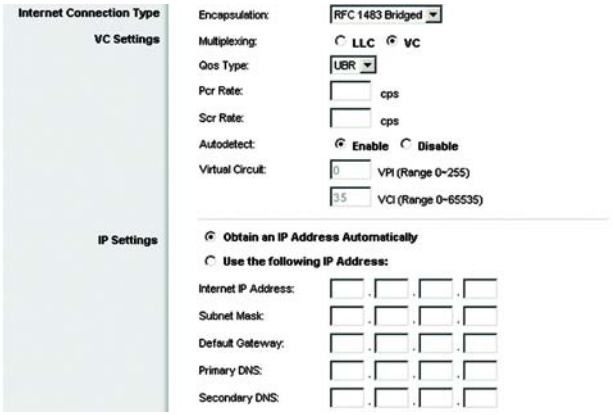


**Abbildung 6-3: „RFC 1483 Bridged“ (RFC 1483-Überbrückung)**

## „RFC 1483 Routed“ (RFC 1483-Weiterleitung)

Wählen Sie zur Verwendung des Modus „RFC 1483 Routed“ die Option **RFC 1483 Routed** (RFC 1483-Weiterleitung) aus.

- **Internet IP Address** (Internet-IP-Adresse): Hierbei handelt es sich um die IP-Adresse des Gateways im WAN bzw. im Internet. Sie erhalten die hier anzugebene IP-Adresse von Ihrem ISP.
- **Subnet Mask** (Subnetzmaske): Hierbei handelt es sich um die Subnetzmaske des Gateways. Sie erhalten die Subnetzmaske von Ihrem ISP.
- **Default Gateway** (Standard-Gateway): Sie erhalten die Standard-Gateway-Adresse von Ihrem ISP. Bei dieser Adresse handelt es sich um die IP-Adresse des ISP-Servers.
- **Primary DNS** (Primärer DNS, erforderlich) und **Secondary DNS** (Sekundärer DNS, optional): Sie erhalten von Ihrem ISP mindestens eine Server-IP-Adresse für das DNS (*Domain Name System*).

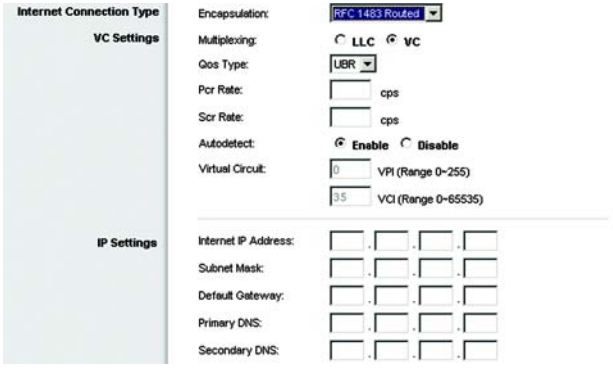


**Abbildung 6-4: „RFC 1483 Routed“ (RFC 1483-Weiterleitung)**

## IPoA

Wenn Sie IPoA (*IP over ATM*) verwenden müssen, wählen Sie die Option **IPoA** aus.

- **Internet IP Address** (Internet-IP-Adresse): Hierbei handelt es sich um die IP-Adresse des Gateways im WAN bzw. im Internet. Sie erhalten die hier anzugebene IP-Adresse von Ihrem ISP.
- **Subnet Mask** (Subnetzmaske): Hierbei handelt es sich um die Subnetzmaske des Gateways. Sie erhalten die Subnetzmaske von Ihrem ISP.
- **Default Gateway** (Standard-Gateway): Sie erhalten die Standard-Gateway-Adresse von Ihrem ISP. Bei dieser Adresse handelt es sich um die IP-Adresse des ISP-Servers.
- **Primary DNS** (Primärer DNS, erforderlich) und **Secondary DNS** (Sekundärer DNS, optional): Sie erhalten von Ihrem ISP mindestens eine Server-IP-Adresse für das DNS (*Domain Name System*).

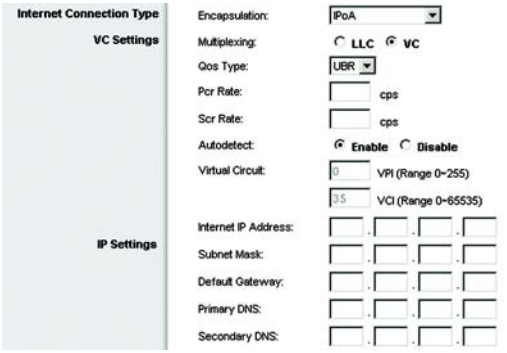


**Abbildung 6-5: IPoA**

## RFC 2516 PPPoE

Einige ISPs mit DSL-Option verwenden PPPoE (*Point-to-Point Protocol over Ethernet*) zur Herstellung von Internetverbindungen. Wenn die Verbindung mit dem Internet über eine DSL-Leitung hergestellt wird, klären Sie mit dem ISP, ob PPPoE verwendet wird. Falls ja, aktivieren Sie die Option **PPPoE**.

- **User Name** (Benutzername) und **Password** (Passwort): Geben Sie den Benutzernamen und das Passwort ein, die Sie von Ihrem ISP erhalten haben.
- **Connect on Demand: Max Idle Time** (Bei Bedarf verbinden: Max. Leerlaufzeit): Sie können das Gateway so konfigurieren, dass die Internetverbindung nach einem bestimmten Zeitraum getrennt wird (maximale Leerlaufzeit). Wenn Ihre Internetverbindung wegen Leerlaufs getrennt wurde, kann das Gateway mithilfe der Option **Connect on Demand** (Bei Bedarf verbinden) Ihre Verbindung automatisch wiederherstellen, sobald Sie wieder versuchen, auf das Internet zuzugreifen. Aktivieren Sie zur Verwendung dieser Option die Optionsschaltfläche **Connect on Demand** (Bei Bedarf verbinden). Geben Sie in das Feld *Max Idle Time* (Max. Leerlaufzeit) die Anzahl der Minuten ein, nach deren Ablauf die Internetverbindung getrennt werden soll.
- **Keep Alive: Redial Period** (Verbindung aufrechterhalten: Wahlwiederholung): Bei Auswahl dieser Option überprüft das Gateway die Internetverbindung in regelmäßigen Abständen. Wenn die Verbindung getrennt wird, wird sie über das Gateway automatisch wieder hergestellt. Aktivieren Sie zur Verwendung dieser Option die Optionsschaltfläche **Keep Alive** (Verbindung aufrechterhalten). Legen Sie im Feld *Redial Period* (Wahlwiederholung) fest, wie oft die Internetverbindung vom Gateway überprüft werden soll. Standardmäßig erfolgt die Wahlwiederholung nach **30** Sekunden.

## RFC 2364 PPPoA

Einige ISPs mit DSL-Option verwenden PPPoA (*Point-to-Point Protocol over ATM*) zur Herstellung von Internetverbindungen. Wenn die Verbindung mit dem Internet über eine DSL-Leitung hergestellt wird, klären Sie mit dem ISP, ob PPPoA verwendet wird. Falls ja, aktivieren Sie die Option **PPPoA**.

- **User Name** (Benutzername) und **Password** (Passwort): Geben Sie den Benutzernamen und das Passwort ein, die Sie von Ihrem ISP erhalten haben.
- **Connect on Demand: Max Idle Time** (Bei Bedarf verbinden: Max. Leerlaufzeit): Sie können das Gateway so konfigurieren, dass die Internetverbindung nach einem bestimmten Zeitraum getrennt wird (maximale Leerlaufzeit). Wenn Ihre Internetverbindung wegen Leerlaufs getrennt wurde, kann das Gateway mithilfe der Option **Connect on Demand** (Bei Bedarf verbinden) Ihre Verbindung automatisch wiederherstellen, sobald Sie wieder versuchen, auf das Internet zuzugreifen. Aktivieren Sie zur Verwendung dieser Option die Optionsschaltfläche **Connect on Demand** (Bei Bedarf verbinden). Geben Sie in das Feld *Max Idle Time* (Max. Leerlaufzeit) die Anzahl der Minuten ein, nach deren Ablauf die Internetverbindung getrennt werden soll.

  **Keep Alive: Redial Period** (Verbindung aufrechterhalten: Wahlwiederholung): Bei Auswahl dieser Option überprüft das Gateway die Internetverbindung in regelmäßigen Abständen. Wenn die Verbindung getrennt wird, wird sie über das Gateway automatisch wieder hergestellt. Aktivieren Sie zur Verwendung dieser Option die Optionsschaltfläche **Keep Alive** (Verbindung aufrechterhalten). Legen Sie im Feld *Redial Period* (Wahlwiederholung) fest, wie oft die Internetverbindung vom Gateway überprüft werden soll. Standardmäßig erfolgt die Wahlwiederholung nach **30** Sekunden.

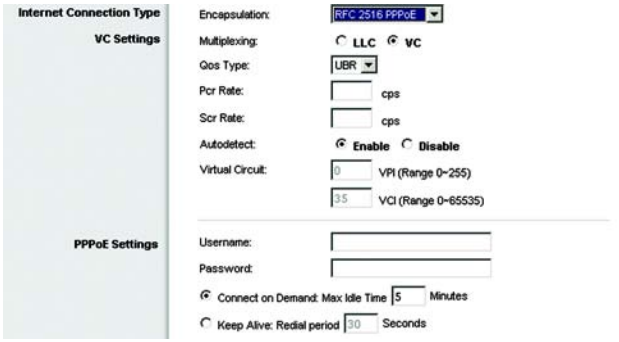


**Abbildung 6-6: RFC 2516 PPPoE**

**WICHTIG:** Damit die Funktion **Connect on Demand** (Bei Bedarf verbinden) ordnungsgemäß arbeitet, schließen Sie alle Internetanwendungen. Ansonsten kann das Gateway unter Umständen die Verbindung nicht beenden, je nachdem, wie oft die Anwendung versucht, eine Verbindung mit dem Internet aufzubauen (z. B. Chat-Programme).

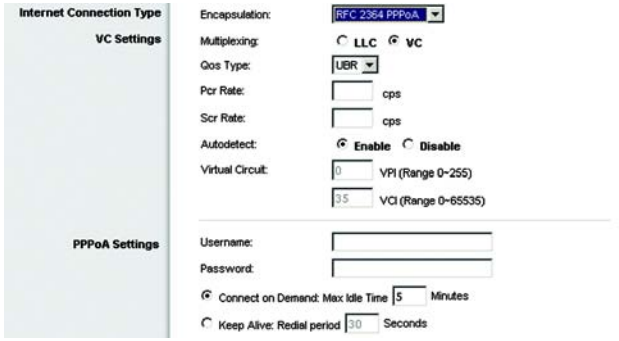


**Abbildung 6-7: RFC 2364 PPPoA**

### „Bridge Mode Only“ (Nur Überbrückungsmodus)

Wenn Sie das Gateway als Überbrückung verwenden (Gateway agiert als Standalone-Modem), wählen Sie die Option **Bridge Mode Only** (Nur Überbrückungsmodus) aus. In diesem Modus sind alle Einstellungen für NAT und Routing deaktiviert.

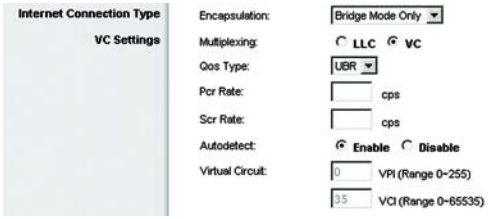


**Abbildung 6-8: „Bridge Mode Only“ (Nur Überbrückungsmodus)**

### „Optional Settings (required by some ISPs)“ (Optionale Einstellungen (für einige ISPs erforderlich))

- **Host Name/Domain Name** (Hostname/Domänenname): In diesen Feldern können Sie einen Hostnamen und Domänennamen für das Gateway eingeben. Für einige ISPs sind diese Namen zu Identifikationszwecken erforderlich. Erfragen Sie bei Ihrem ISP, ob Ihr Breitband-Internetdienst mit einem Host- und Domänennamen konfiguriert wurde. In den meisten Fällen können diese Felder leer gelassen werden.
- **MTU** und **Size** (Größe): Mit der MTU-Einstellung (*Maximum Transmission Unit*, Maximale Übertragungseinheit) wird die maximale Paketgröße festgelegt, die zur Netzwerkübertragung zugelassen ist. Wählen Sie **Manual** (Manuell) aus, und geben Sie im Feld *Size* (Größe) den gewünschten Wert ein. Es wird empfohlen, einen Wert zwischen 1200 und 1500 einzugeben. Die maximale Übertragungseinheit (MTU) wird standardmäßig automatisch konfiguriert.

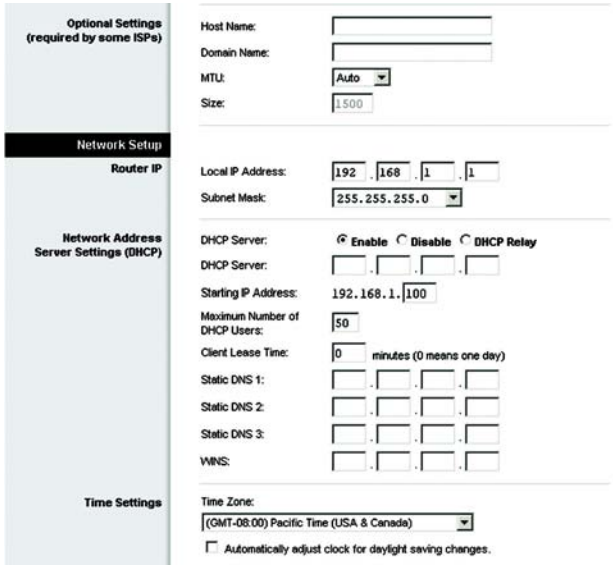


**Abbildung 6-9: „Optional Settings“ (Optionale Einstellungen)**

### „Network Setup“ (Netzwerkeinrichtung)

- **Router IP** (IP-Adresse des Routers): Die Werte für die lokale IP-Adresse und Subnetzmaske des Gateways sind hier aufgeführt. In den meisten Fällen können die Standardwerte beibehalten werden.
  - **Local IP Address** (Lokale IP-Adresse): Der Standardwert ist **192.168.1.1**.
  - **Subnet Mask** „Subnetzmaske“: Der Standardwert ist **255.255.255.0**.
- **Network Address Server Settings (DHCP)** (Einstellungen des Netzwerkadressenservers (DHCP)): In diesem Bereich können Sie die DHCP-Einstellungen (*Dynamic Host Configuration Protocol*) des Gateways konfigurieren.
  - **DHCP Server** (DHCP-Server): Ein DHCP-Server (*Dynamic Host Configuration Protocol*) weist jedem Computer im Netzwerk automatisch eine IP-Adresse zu. Wenn Sie nicht schon über eine IP-Adresse verfügen, ist es äußerst empfehlenswert, das Gateway als DHCP-Server aktiviert zu lassen. Das Gateway kann auch im DHCP-Relay-Modus verwendet werden. (Diese Einstellung ist nicht bei allen Kapselungstypen verfügbar.)
  - **DHCP Server** (DHCP-Server): Wenn Sie für die Einstellung *DHCP Server* (DHCP-Server) den DHCP-Relay-Modus aktivieren, geben Sie die IP-Adresse für den DHCP-Relay-Server in den entsprechenden Feldern ein. (Diese Einstellung ist nicht bei allen Kapselungstypen verfügbar.)

- **Starting IP Address** (Start-IP-Adresse): Geben Sie einen Wert ein, mit dem der DHCP-Server beim Zuweisen von IP-Adressen beginnen soll. Der Wert muss mindestens 192.168.1.2 betragen, da die Standard-IP-Adresse für das Gateway **192.168.1.1** ist.

- **Maximum Number of DHCP Users** (Maximale Anzahl der DHCP-Benutzer): Geben Sie die maximale Anzahl der Benutzer bzw. Clients ein, denen eine IP-Adresse zugewiesen werden kann. Diese Zahl hängt von der eingegebenen Start-IP-Adresse ab.

- **Client Lease Time** (Client-Leasedauer): Bei der Client-Leasedauer handelt es sich um den Zeitraum, in dem ein Computer über seine aktuelle dynamische IP-Adresse eine Verbindung mit dem Gateway herstellen kann. Geben Sie in Minuten an, wie lange diese dynamische IP-Adresse dem Computer zugewiesen bleiben soll.

- **Static DNS 1-3** (Statisches DNS 1-3): Mit dem DNS (*Domain Name System*) übersetzt das Internet Domänen- oder Website-Namen in Internetadressen oder URLs. Sie erhalten von Ihrem ISP mindestens eine IP-Adresse für den DNS-Server. Hier können Sie bis zu drei IP-Adressen für den DNS-Server eingeben. Das Gateway verwendet diese für einen schnelleren Zugriff auf laufende DNS-Server.

- **WINS**: Mithilfe von WINS (*Windows Internet Naming Service*) werden NetBIOS-Namen in IP-Adressen umgewandelt. Wenn Sie einen WINS-Server verwenden, geben Sie hier die IP-Adresse des Servers ein. Andernfalls lassen Sie dieses Feld leer.

- **Time Setting** (Zeiteinstellung): Wählen Sie die entsprechende Zeitzone für den Standort des Gateways aus. Aktivieren Sie gegebenenfalls das Kontrollkästchen **Automatically adjust clock for daylight saving changes** (Uhr automatisch an Zeitumstellung anpassen).

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

## Registerkarte „DDNS“

Das Gateway verfügt über die Funktion DDNS (*Dynamic Domain Name System*). Mit DDNS können Sie einer dynamischen Internet-IP-Adresse einen festen Host- und Domänennamen zuweisen. Dies kann sich für das Hosting Ihrer eigenen Website, Ihres FTP-Servers oder anderer Server hinter dem Gateway als nützlich erweisen.

Bevor Sie diese Funktion verwenden können, müssen Sie sich für den DDNS-Dienst unter www.dyndns.org oder www.tzo.com anmelden.

**Abbildung 6-10: DDNS – DynDNS.org**

### DDNS

**DDNS Service** (DDNS-Dienst): Wenn der verwendete DDNS-Dienst von DynDNS.org zur Verfügung gestellt wird, wählen Sie im Dropdown-Menü die Option **DynDNS.org** aus. Wenn der verwendete DDNS-Dienst von TZO.com zur Verfügung gestellt wird, wählen Sie im Dropdown-Menü die Option **TZO.com** aus. Zum Deaktivieren des DDNS-Dienstes wählen Sie **Disabled** (Deaktiviert) aus.

### DynDNS.org

- **User Name** (Benutzername), **Password** (Passwort) und **Host Name** (Hostname): Geben Sie den Benutzernamen, das Passwort und den Hostnamen des mithilfe von DynDNS.org festgelegten Kontos an.
- **Status**: Hier wird der Status der Verbindung zum DDNS-Dienst aufgeführt.
- **Connect** (Verbinden): Klicken Sie auf die Schaltfläche **Connect** (Verbinden), um die Verbindung mit dem DDNS-Dienst herzustellen.

### TZO.com

- **E-mail Address** (E-Mail-Adresse), **Password** (Passwort) und **Domain Name** (Domänenname): Geben Sie die E-Mail-Adresse, das Passwort und den Domänennamen des Kontos ein, das Sie bei TZO eingerichtet haben.
- **Status**: Hier wird der Status der Verbindung zum DDNS-Dienst aufgeführt.
- **Connect** (Verbinden): Klicken Sie auf die Schaltfläche **Connect** (Verbinden), um die Verbindung mit dem DDNS-Dienst herzustellen.

**Abbildung 6-11: DDNS – TZO.com**

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

## Registerkarte „Advanced Routing“ (Erweitertes Routing)

Über das Fenster *Advanced Routing* (Erweitertes Routing) können Sie die Einstellungen für NAT sowie für das dynamische und statische Routing konfigurieren.

### „Advanced Routing“ (Erweitertes Routing)

- **Operating Mode** (Betriebsmodus): In diesem Bereich können Sie die allgemeinen Routing-Einstellungen des Gateways konfigurieren.
    - **NAT**: Bei NAT handelt es sich um eine Sicherheitsfunktion, die standardmäßig aktiviert ist. Das Gateway kann über diese Funktion IP-Adressen des lokalen Netzwerks in eine andere IP-Adresse für die Internetnutzung umwandeln. Um NAT zu deaktivieren, klicken Sie auf das Optionsfeld **Disabled** (Deaktiviert).
- **Dynamic Routing** (Dynamisches Routing): Mit der Option **Dynamic Routing** (Dynamisches Routing) kann das Gateway automatisch an physische Änderungen in der Netzwerkanordnung angepasst werden. Bei Verwendung von RIP legt das Gateway die Route der Netzwerkpakete auf Grundlage der geringsten Anzahl der Gateways zwischen Quelle und Ziel fest. Über das RIP-Protokoll werden in regelmäßigen Abständen Routing-Informationen an andere Gateways im Netzwerk gesendet.
    - **RIP**: Bei mehreren Routern empfiehlt es sich, RIP (*Routing Information Protocol*) zu verwenden, damit die Router untereinander Routing-Informationen austauschen können. Klicken Sie zur Verwendung von RIP auf das Optionsfeld **Enabled** (Aktiviert). Behalten Sie andernfalls die Standardeinstellung **Disabled** (Deaktiviert) bei.
    - **RIP Send Packet Version** (RIP-Version für gesendete Pakete): Wählen Sie die gewünschte Protokollversion aus: **RIPv1** oder **RIPv2**.
    - **RIP Recv Packet Version** (RIP-Version für erhaltene Pakete): Wählen Sie die gewünschte Protokollversion aus: **RIPv1** oder **RIPv2**.
- **Static Routing** (Statisches Routing): Wenn das Gateway an mehr als einem Netzwerk angeschlossen ist, muss u. U. zwischen den Gateways eine statische Route eingerichtet werden. Eine statische Route ist ein vordefinierter Pfad, über den Netzwerkinformationen an einen bestimmten Host oder ein bestimmtes Netzwerk übertragen werden. Ändern Sie die folgenden Einstellungen, um eine statische Route zu erstellen:
    - **Select set number** (Set-Nummer auswählen): Wählen Sie im Dropdown-Menü die Nummer der statischen Route aus. Das Gateway unterstützt bis zu 20 Einträge für statische Routeneinträge. Wenn Sie eine Route löschen möchten, wählen Sie den entsprechenden Eintrag aus, und klicken Sie auf die Schaltfläche **Delete This Entry** (Diesen Eintrag löschen).

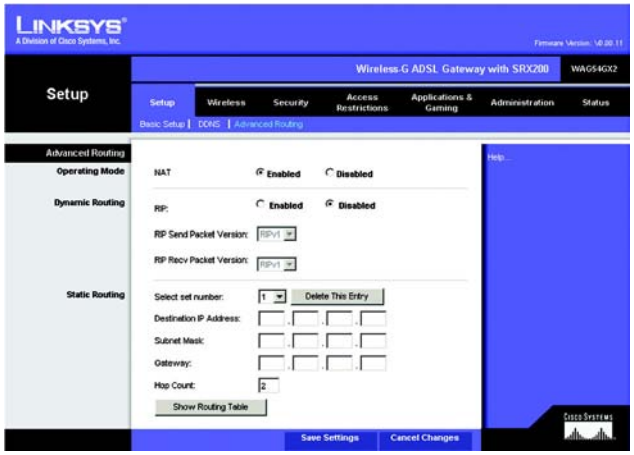


**Abbildung 6-12: „Advanced Routing“ (Erweitertes Routing)**

- **Destination IP Address** (Ziel-IP-Adresse): Bei der Ziel-IP-Adresse handelt es sich um die Adresse des entfernten Netzwerks bzw. Hosts, dem Sie eine statische Route zuweisen möchten. Geben Sie die IP-Adresse des Hosts ein, für den Sie eine statische Route erstellen möchten. Wenn Sie eine Route zu einem gesamten Netzwerk erstellen, vergewissern Sie sich, dass für den Netzwerkbereich der IP-Adresse der Wert **0** festgelegt ist.

- **Subnet Mask** (Subnetzmaske): Geben Sie die Subnetzmaske (auch Netzwerkmaske genannt) ein, mit der festgelegt wird, welcher Bereich einer IP-Adresse der Netzwerkbereich und welcher Bereich der Hostbereich ist.

- **Gateway**: Geben Sie die IP-Adresse des Gateway-Geräts ein, das eine Verbindung zwischen dem Gateway und dem entfernten Netzwerk bzw. Host ermöglicht.

- **Hop Count** (Anzahl der Gateways): Gibt die Anzahl der Gateways bis zu den einzelnen Knoten an, bevor das Ziel erreicht wird (max. 16 Gateways). Geben Sie die gewünschte Anzahl im entsprechenden Feld ein.

- **Show Routing Table** (Routing-Tabelle anzeigen): Klicken Sie auf die Schaltfläche **Show Routing Table** (Routing-Tabelle anzeigen), um ein Fenster zu öffnen, in dem die Weiterleitung von Daten im lokalen Netzwerk angezeigt wird. Für jede Route wird die IP-Adresse des Ziel-LANs, die Subnetzmaske, das Gateway und die Schnittstelle angezeigt. Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die Daten zu aktualisieren. Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum Fenster zurückzukehren.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

**Abbildung 6-13: „Routing Table“ (Routing-Tabelle)**

# Registerkarte „Wireless“

## Registerkarte „Basic Wireless Settings“ (Grundlegende Wireless-Einstellungen)

In diesem Fenster können Sie den Wireless-Netzwerkmodus und die Sicherheit im Wireless-Netzwerkbetrieb festlegen.

### „Wireless Network“ (Wireless-Netzwerk)

- **Wireless Network Mode** (Wireless-Netzwerkmodus): Wenn sich sowohl 802.11g- als auch 802.11b-Geräte im Netzwerk befinden, behalten Sie die Standardeinstellung **Mixed** (Gemischt) bei. Wenn ausschließlich 802.11g-Geräte vorhanden sind, wählen Sie **G-Only** (Nur G) aus. Wenn ausschließlich 802.11b-Geräte vorhanden sind, wählen Sie **B-Only** (Nur B) aus. Um das Wireless-Netzwerk zu deaktivieren, wählen Sie **Disable** (Deaktivieren).

- **Wireless Network Name (SSID)** (Wireless-Netzwerkname (SSID)): Geben Sie in diesem Feld den Namen für das Wireless-Netzwerk ein. Bei der SSID handelt es sich um den Netzwerknamen, der von allen Geräten im drahtlosen Netzwerk verwendet wird. Sie muss für alle Geräte im Wireless-Netzwerk identisch sein. Für die maximal 32 Zeichen lange SSID dürfen alle alphanumerischen Zeichen der Tastatur verwendet werden. Es wird nach Groß- und Kleinschreibung unterschieden. Sie sollten die standardmäßige SSID (linksys) in einen eindeutigen Namen Ihrer Wahl ändern.

- **Wireless Channel** (Wireless-Kanal): Wählen Sie aus der Liste den Ihren Netzwerkeinstellungen entsprechenden Kanal aus. Eine korrekte Funktion Ihres Wireless-Netzwerks ist nur gewährleistet, wenn die Übertragung für alle Geräte über denselben Kanal erfolgt. Die Wireless-Computer oder -Clients erkennen den Wireless-Kanal des Gateways automatisch.

- **Wireless SSID Broadcast** (Wireless-SSID-Übertragung): Wenn Wireless-Computer oder -Clients im lokalen Netzwerk nach Wireless-Netzwerken suchen, mit denen sie eine Verbindung herstellen können, erkennen sie die vom Gateway übertragene SSID. Wenn die SSID des Gateways übertragen werden soll, behalten Sie die Standardeinstellung **Enable** (Aktivieren) bei. Wenn die SSID des Gateways nicht übertragen werden soll, wählen Sie **Disable** (Deaktivieren) aus.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

**Abbildung 6-14: „Basic Wireless Settings“ (Grundlegende Wireless-Einstellungen)**

## Registerkarte „Wireless Security“ (Sicherheit im Wireless-Netzwerkbetrieb)

Mit den Wireless-Sicherheitseinstellungen wird die Sicherheit des Wireless-Netzwerks konfiguriert. Das Gateway unterstützt sechs Optionen für die Sicherheit im Wireless-Netzwerkbetrieb: **WPA-Personal**, **WPA2-Personal**, **WPA2-Mixed** (WPA2 Gemischt), WPA Enterprise, WPA2 Enterprise und **WEP**. WPA steht für *Wi-Fi Protected Access*. Dies ist ein höherer Sicherheitsstandard als die WEP-Verschlüsselung (*Wired Equivalent Privacy*). WPA2 ist eine komplexere, sicherere Version von WPA. WPA Enterprise und WPA2 Enterprise verwenden RADIUS (Remote Authentication Dial-In User Service) für die Authentifizierung. Im Folgenden werden diese Sicherheitsstandards kurz erläutert. Genauere Anweisungen zur Konfiguration der Sicherheit im Wireless-Netzwerkbetrieb des Gateways finden Sie in „Anhang B: Sicherheit im Wireless-Netzwerkbetrieb“.

Um die Option zur Sicherheit im Wireless-Netzwerkbetrieb zu deaktivieren, wählen Sie im Dropdown-Menü *Security Mode* (Sicherheitsmodus) die Option **Disable** (Deaktivieren) aus.

- **Security Mode** (Sicherheitsmodus): Wählen Sie den im Netzwerk zu verwendenden Modus aus: **WPA-Personal**, **WPA2-Personal**, **WPA2-Mixed** (WPA2 Gemischt), **WPA Enterprise**, **WPA2 Enterprise** oder **WEP**. Wenn Geräte für **WPA-Personal** und **WPA2-Personal** verwendet werden, wählen Sie **WPA2-Mixed** (WPA2 Gemischt) aus.

### WPA-Personal

- **Encryption** (Verschlüsselung): Wählen Sie die gewünschte Verschlüsselungsmethode aus: **TKIP** oder **AES**. (AES bietet eine stärkere Verschlüsselung als TKIP.)
- **Passphrase**: Geben Sie den Schlüssel ein, der vom Gateway und von den anderen Netzwerkgeräten gemeinsam verwendet wird. Er muss aus 8 bis 63 Zeichen bestehen.
- **Key Renewal** (Schlüsselerneuerung): Geben Sie den Zeitraum für die Schlüsselerneuerung ein. Dieser gibt an, wie oft das Gateway die dynamischen Verschlüsselungsschlüssel ändern soll.

Klicken Sie nach dem Vornehmen aller Änderungen in diesem Fenster auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu speichern, oder klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen), um die Änderungen rückgängig zu machen. Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

### WPA2-Personal

- **Encryption** (Verschlüsselung): Es wird automatisch **AES** ausgewählt.
- **Passphrase**: Geben Sie den Schlüssel ein, der vom Gateway und von den anderen Netzwerkgeräten gemeinsam verwendet wird. Er muss aus 8 bis 63 Zeichen bestehen.
- **Key Renewal** (Schlüsselerneuerung): Geben Sie den Zeitraum für die Schlüsselerneuerung ein. Dieser gibt an, wie oft das Gateway die dynamischen Verschlüsselungsschlüssel ändern soll.

**Abbildung 6-15: „Wireless Security“ (Wireless-Sicherheit) – „WPA-Personal“**

**WICHTIG:** Wenn Sie die Wireless-Sicherheit verwenden, MUSS jedes Gerät im Wireless-Netzwerk dieselbe Methode für die Wireless-Sicherheit und denselben gemeinsamen Schlüssel verwenden, damit das Wireless-Netzwerk ordnungsgemäß funktioniert. Wenn Geräte für **WPA-Personal** und **WPA2-Personal** verwendet werden, sollten Sie **WPA2-Mixed** (WPA2 Gemischt) auswählen. Sie können WPA und WPA2 Enterprise mischen, nicht jedoch Personal und Enterprise, Personal und WEP bzw. Enterprise und WEP.

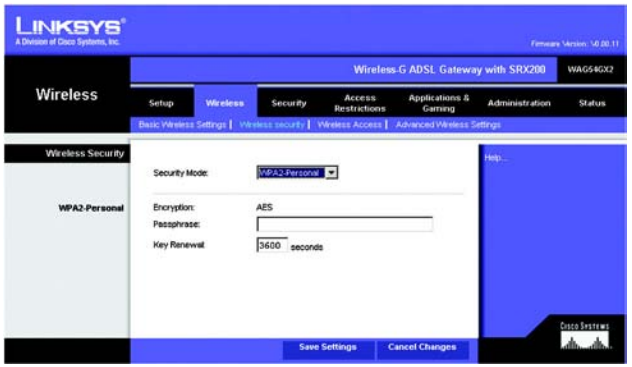


**Abbildung 6-16: „Wireless Security“ (Wireless-Sicherheit) – „WPA2-Personal“**

Klicken Sie nach dem Vornehmen aller Änderungen in diesem Fenster auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu speichern, oder klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen), um die Änderungen rückgängig zu machen. Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

### „WPA2-Mixed“ (WPA2 Gemischt)

- **Encryption** (Verschlüsselung): Es wird automatisch **TKIP + AES** ausgewählt, damit beide Methoden verfügbar sind.
- **Passphrase**: Geben Sie den Schlüssel ein, der vom Gateway und von den anderen Netzwerkgeräten gemeinsam verwendet wird. Er muss aus 8 bis 63 Zeichen bestehen.
- **Key Renewal** (Schlüsselerneuerung): Geben Sie den Zeitraum für die Schlüsselerneuerung ein. Dieser gibt an, wie oft das Gateway die dynamischen Verschlüsselungsschlüssel ändern soll.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

**Abbildung 6-17: „Wireless Security“ (Wireless-Sicherheit) – „WPA2-Mixed“ (WPA2 Gemischt)**

### „WPA Enterprise“ (WPA-Enterprise)

Bei der Verschlüsselungsmethode WPA Enterprise wird WPA in Kombination mit einem RADIUS-Server verwendet. (Diese Methode sollte nur dann eingesetzt werden, wenn das Gateway mit einem RADIUS-Server verbunden ist.)

- **RADIUS Server Address** (RADIUS-Server-Adresse): Geben Sie die IP-Adresse des RADIUS-Servers ein.
- **RADIUS Port** (RADIUS-Port): Geben Sie die Port-Nummer des RADIUS-Servers ein.
- **Shared Key** (Freigegebener Schlüssel): Geben Sie den Schlüssel ein, der vom Gateway und dem zugehörigen RADIUS-Server gemeinsam verwendet wird.
- **Key Renewal Timeout** (Wartezeit für Schlüsselerneuerung): Geben Sie den Zeitraum für die Schlüsselerneuerung ein. Dieser gibt an, wie oft das Gateway die dynamischen Verschlüsselungsschlüssel ändern soll.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

**Abbildung 6-18: „Wireless Security“ (Wireless-Sicherheit) – „WPA Enterprise“**

### WPA2 Enterprise

Bei der Verschlüsselungsmethode **WPA2 Enterprise** wird WPA2 in Kombination mit einem RADIUS-Server verwendet. (Diese Methode sollte nur dann eingesetzt werden, wenn das Gateway mit einem RADIUS-Server verbunden ist.)

- **RADIUS Server Address** (RADIUS-Server-Adresse): Geben Sie die IP-Adresse des RADIUS-Servers ein.
- **RADIUS Port** (RADIUS-Port): Geben Sie die Port-Nummer des RADIUS-Servers ein.
- **Shared Key** (Freigegebener Schlüssel): Geben Sie den Schlüssel ein, der vom Gateway und dem zugehörigen RADIUS-Server gemeinsam verwendet wird.
- **Key Renewal Timeout** (Wartezeit für Schlüsselerneuerung): Geben Sie den Zeitraum für die Schlüsselerneuerung ein. Dieser gibt an, wie oft das Gateway die dynamischen Verschlüsselungsschlüssel ändern soll.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

**Abbildung 6-19: „Wireless Security“ (Wireless-Sicherheit) – „WPA2 Enterprise“**

### WEP

- **Encryption** (Verschlüsselung): Wählen Sie die entsprechende Verschlüsselungsebene aus: **64 Bit** oder **128 Bit**. Eine höhere Verschlüsselungsebene bedeutet mehr Sicherheit.
- **Passphrase**: Sie können anstelle der manuellen Eingabe von WEP-Schlüsseln eine Passphrase verwenden. Hierbei wird zwischen Groß- und Kleinschreibung unterschieden, und die Länge von 32 alphanumerischen Zeichen darf nicht überschritten werden. (Die Passphrase ist nur mit Wireless-Produkten von Linksys kompatibel und kann nicht mit dem Windows XP-Dienstprogramm zur konfigurationsfreien Verbindung verwendet werden. Wenn Sie mit Wireless-Produkten anderer Hersteller oder mithilfe der drahtlosen Verbindung unter Windows XP kommunizieren möchten, notieren Sie die generierten WEP-Schlüssel, und geben Sie den entsprechenden Schlüssel manuell am Wireless-Computer bzw. im Client ein.) Wenn Sie eine Passphrase verwenden möchten, geben Sie sie im Feld *Passphrase* ein, und klicken Sie auf die Schaltfläche **Generate** (Erstellen).
- **WEP Key 1** (WEP-Schlüssel 1) bis **WEP Key 4** (WEP-Schlüssel 4): Wenn Sie keine Passphrase verwenden, geben Sie manuell einen Wertesatz ein. (Lassen Sie ein Schlüsselfeld nicht leer, und geben Sie nicht in allen Schlüsselfeldern den Wert 0 ein, da es sich hierbei nicht um gültige Schlüsselwerte handelt.) Wenn Sie eine 40/64-Bit-WEP-Verschlüsselung verwenden, muss die Schlüssellänge genau 10 Hexadezimalziffern betragen. Wenn Sie eine 128-Bit-WEP-Verschlüsselung verwenden, muss die Schlüssellänge genau 26 hexadezimale Zeichen betragen. Gültige hexadezimale Zeichen sind Zeichen von „0“ bis „9“ und von „A“ bis „F“.

**Abbildung 6-20: „Wireless Security“ (Wireless-Sicherheit) – „WEP“**

- **TX Key** (TX-Schlüssel): Wählen Sie eine Standardnummer für den Übertragungsschlüssel aus, um den zu verwendenden WEP-Schlüssel anzugeben.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

## Registerkarte „Wireless Access“ (Wireless-Zugriff)

### „Wireless Network Access“ (Wireless-Netzwerkzugriff)

**Wireless Network Access** (Wireless-Netzwerkzugriff): Aktivieren Sie **Allow All** (Alle zulassen), wenn allen Computern der Zugriff auf das Wireless-Netzwerk ermöglicht werden soll. Soll der Zugriff eingeschränkt werden, wählen Sie **Restrict Access** (Zugriff beschränken) und anschließend zum Verweigern des Zugriffs für bestimmte Computer die Option **Prevent** (Verweigern) oder zum Gestatten des Zugriffs für bestimmte Computer die Option **Permit only** (Nur Zugriff) aus. Klicken Sie auf die Schaltfläche **Update Filter List** (Filterliste aktualisieren). Daraufhin wird das Fenster *Mac Address Filter List* (MAC-Adressen-Filterliste) angezeigt.

Geben Sie die MAC-Adressen der Computer ein, die Sie festlegen möchten. Wenn Sie eine Liste der MAC-Adressen für Wireless-Computer oder -Clients anzeigen möchten, klicken Sie auf die Schaltfläche **Wireless Client MAC List** (MAC-Liste der Wireless-Clients).

Im Fenster *Wireless Client List* (Liste der Wireless-Clients) sind die MAC-Adressen der Wireless-Geräte aufgeführt. Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), damit die aktuellsten Informationen angezeigt werden. Wenn der MAC-Adressen-Filterliste ein bestimmter Computer hinzugefügt werden soll, aktivieren Sie das Kontrollkästchen **Enable MAC Filter** (MAC-Filter aktivieren), und klicken Sie anschließend auf die Schaltfläche **Update Filter List** (Filterliste aktualisieren). Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum Fenster *MAC Address Filter List* (MAC-Adressen-Filterliste) zurückzukehren.

Klicken Sie im Fenster *MAC Address Filter List* (MAC-Adressen-Filterliste) auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Liste zu speichern, oder auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen), um die Eingaben zu löschen.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

**Abbildung 6-21: „Wireless Access“ (Wireless-Zugriff)**

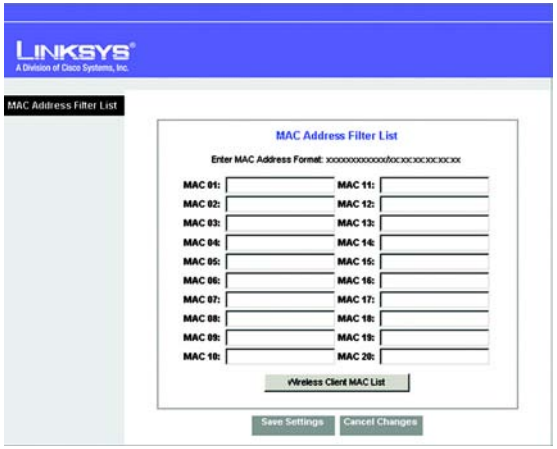


**Abbildung 6-22: „MAC Address Filter List“ (MAC-Adressen-Filterliste)**

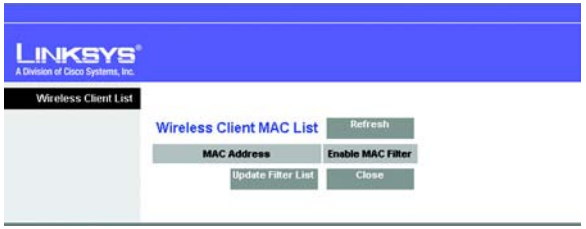


**Abbildung 6-23: „Wireless Client MAC List“ (MAC-Liste der Wireless-Clients)**

## Registerkarte „Advanced Wireless Settings“ (Erweiterte Wireless-Einstellungen)

In diesem Fenster können Sie auf die erweiterten Wireless-Funktionen zugreifen.

### „Advanced Wireless“ (Erweitertes Wireless)

„Wireless-G Settings“ (Wireless-G-Einstellungen)

Auf dieser Registerkarte werden die erweiterten Wireless-Funktionen des Gateways eingerichtet. Diese Einstellungen sollten nur von einem erfahrenen Administrator angepasst werden, da falsche Einstellungen die Leistung des Routers im Wireless-Betrieb beeinträchtigen können.

**Abbildung 6-24: „Advanced Wireless Settings“ (Erweiterte Wireless-Einstellungen)**

- **Basic Rate Set** (Eingestellte Grundrate): Die eingestellte Grundrate stellt einen Satz von Raten dar, mit denen das Gateway Übertragungen ausführen kann. (Wenn Sie die Datenübertragungsrate des Gateways festlegen möchten, konfigurieren Sie die Einstellung **Transmission Rate** (Übertragungsrate).) Das Gateway teilt anderen Wireless-Geräten im Netzwerk seine eingestellte Grundrate mit, sodass bekannt ist, welche Raten unterstützt werden. Der Gateway gibt außerdem bekannt, dass automatisch die optimale Übertragungsrate ausgewählt wird. In den meisten Fällen sollten Sie die Standardeinstellung übernehmen, also **Default (1-2-5.5-11)** (Standard (1-2-5.5-11). Weitere verfügbare Optionen sind **1-2Mbps** (1-2 MBit/s) für die Verwendung mit älterer Wireless-Technologie und **All** (Alle), wenn das Gateway bei allen standardmäßigen Wireless-Raten Übertragungen ausführen kann.

- **Transmission Rate** (Übertragungsrate): Die Datenübertragungsrate sollte gemäß der Geschwindigkeit des Wireless-Netzwerks eingestellt werden. Sie können aus einer Reihe von Übertragungsgeschwindigkeiten auswählen oder auch die Option **Auto** (Automatisch) aktivieren, mit der das Gateway automatisch die schnellstmögliche Datenrate verwendet und die Funktion für automatisches Fallback aktiviert wird. Mit der Funktion für automatisches Fallback wird die optimale Verbindungsgeschwindigkeit zwischen dem Gateway und einem Wireless-Client ermittelt. Die Standardeinstellung lautet **Auto** (Automatisch).

- **CTS Protection Mode** (CTS-Schutzmodus): Behalten Sie die Standardeinstellung **Auto** (Automatisch) für die Option **CTS Protection Mode** (CTS-Schutzmodus; CTS = Clear-To-Send) bei, damit der CTS-Schutzmodus verwendet wird, wenn Ihre Wireless-G-Produkte in einer Umgebung mit hohem 802.11b-Datenverkehr keine Übertragungen an den Gateway ausführen können. Diese Funktion verbessert zwar die Fähigkeit des Gateways, alle Wireless-G-Übertragungen zu empfangen, verringert jedoch auch beträchtlich seine Leistung.

- **Beacon Interval** (Beacon-Intervall): Ein Beacon ist eine Paketübertragung des Gateways zur Synchronisierung des Wireless-Netzwerks.**Beacon Interval** (Beacon-Intervall): Der Standardwert ist **100**. Geben Sie einen Wert zwischen 1 und 65.535 Millisekunden ein. Der Wert des Beacon-Intervalls gibt das Sendeintervall des Beacons an. Ein Beacon ist eine Paketübertragung des Gateways zur Synchronisierung des Wireless-Netzwerks.

- **DTIM Interval** (DTIM-Intervall): Der Wert (zwischen 1 und 255) gibt das Intervall der DTIM (*Delivery Traffic Indication Message*) an. Ein DTIM-Feld ist ein Zeitkontrollfeld, das die Clients über das nächste Fenster informiert, in dem nach Broadcast- und Multicast-Meldungen gesucht wird. Wenn das Gateway Broadcast- oder Multicast-Meldungen für die zugewiesenen Clients gepuffert hat, sendet er die nächste DTIM mit einem DTIM-Intervallwert. Die zugewiesenen Clients empfangen das Beacon-Signal und sind zum Empfang der Broadcast- und Multicast-Meldungen bereit. Der Standardwert lautet **1**.

- **Fragmentation Threshold** (Fragmentierungsschwelle): Dieser Wert gibt die maximale Größe eines Pakets an, bevor die Daten in mehrere Pakete unterteilt werden. Wenn Sie eine hohe Paketfehlerrate wahrnehmen, können Sie die Fragmentierungsschwelle leicht anheben. Liegt die Fragmentierungsschwelle zu niedrig, kann dies zu einer Herabsetzung der Netzwerkleistung führen. Es wird empfohlen, den Standardwert nur geringfügig zu senken. In den meisten Fällen sollte er beim Standardwert **2346** belassen werden.

- **RTS Threshold** (RTS-Schwelle): Bei einem schwankenden Datenfluss wird eine nur geringfügige Senkung empfohlen. Wenn ein Netzwerkpaket kleiner als die voreingestellte RTS-Schwellengröße ist, wird der RTS/CTS-Mechanismus nicht aktiviert. Das Gateway sendet RTS-Blöcke (*RTS = Request to Send*) an eine bestimmte Empfangsstation und handelt das Senden eines Daten-Blocks aus. Nach dem Empfang eines RTS-Blocks antwortet die Wireless-Station mit einem CTS-Block (*CTS = Clear to Send*), um das Recht, mit der Übertragung zu beginnen, zu bestätigen. Dieser Wert sollte bei dem Standardwert **2346** belassen werden.

- **Preamble Type** (Präambeltyp): Die Präambel legt die Länge des CRC-Blocks (*Cyclic Redundancy Check*) zur Kommunikation des Gateways mit den Wireless-Roaming-Clients fest. (In Bereichen mit hohem Netzwerkverkehr sollte der kürzere Präambeltyp verwendet werden.) Wählen Sie den geeigneten Präambeltyp aus: **Long** (Lang; Standardeinstellung) oder **Short** (Kurz).

- **Network Density** (Netzwerkdichte): Diese Einstellung bestimmt den Übertragungs- und Empfangsbereich des Gateways. Wählen Sie eine der folgenden Einstellungen aus: **Low** (Niedrig; größere Reichweite), **Medium** (Mittel; mittelgroße Reichweite) oder **High** (Hoch; kleinere Reichweite). Die Einstellung **Low** (Niedrig) wird empfohlen, wenn nur wenige Wireless-Netzwerke in Ihrer Arbeitsumgebung betrieben werden, die Einstellung **High** (Hoch) entsprechend dann, wenn starker Datenverkehr in nahe gelegenen Wireless-Netzwerken vorliegt. Die Einstellung **Medium** (Mittel) bildet den Mittelweg bei der Reichweite. Die Standardeinstellung lautet **Low** (Niedrig).

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

# Registerkarte „Security“ (Sicherheit)

## Registerkarte „Firewall“

Sie können die Firewall aktivieren oder deaktivieren, Filter zum Blockieren bestimmter Internetdatentypen auswählen und anonyme Internet-Anfragen blockieren. Verwenden Sie diese Funktionen, um die Sicherheit des Netzwerks zu erhöhen.

### Firewall

- **SPI Firewall Protection** (SPI-Firewall-Schutz): Die Firewall-Funktion SPI (*Stateful Packet Inspection*) erhöht die Sicherheit des Netzwerks. Klicken Sie zur Verwendung dieser Funktion auf **Enable** (Aktivieren). Wenn die Firewall nicht verwendet werden soll, klicken Sie auf **Disable** (Deaktivieren).

„Additional Filters“ (Zusätzliche Filter)

- **Filter Proxy** (Proxy filtern): Die Verwendung von WAN-Proxyservern kann die Sicherheit des Gateways beeinträchtigen. Wenn Sie die Proxyfilterung verweigern, wird der Zugriff auf alle WAN-Proxyserver deaktiviert. Aktivieren Sie zum Verwenden der Proxy-Filterung das entsprechende Kontrollkästchen.
- **Filter Cookies** (Cookies filtern): Bei einem Cookie handelt es sich um Daten, die auf einem Computer gespeichert sind und von Websites beim Zugriff auf diese Sites verwendet werden. Aktivieren Sie zum Verwenden der Cookie-Filterung das entsprechende Kontrollkästchen.
- **Filter Java Applets** (Java-Applets filtern): Bei Java handelt es sich um eine Programmiersprache für Websites. Wenn Sie Java-Applets ablehnen, haben Sie möglicherweise keinen Zugriff auf Websites, die mit dieser Programmiersprache erstellt wurden. Aktivieren Sie zum Verwenden der Java Applet-Filterung das entsprechende Kontrollkästchen.
- **Filter ActiveX** (ActiveX filtern): Bei ActiveX handelt es sich um eine Programmiersprache für Websites. Wenn Sie ActiveX ablehnen, haben Sie möglicherweise keinen Zugriff auf Websites, die mit dieser Programmiersprache erstellt wurden. Aktivieren Sie zum Verwenden der ActiveX-Filterung das entsprechende Kontrollkästchen.

„Block WAN Requests“ (WAN-Anfragen blockieren)

- **Block Anonymous Internet Requests** (Anonyme Internet-Anfragen blockieren): Mit dieser Option können Sie Ihr Netzwerk vor Ping-Angriffen oder dem Erkennen durch andere Internetbenutzer schützen. Darüber hinaus können Sie mit dieser Option die Sicherheit des Netzwerks erhöhen, indem die Netzwerk-Ports nicht angezeigt werden und das Netzwerk vor Angreifern aus dem Internet besser geschützt ist. Aktivieren Sie die Option **Block Anonymous Internet Requests** (Anonyme Internet-Anfragen blockieren), um anonyme Internet-Anfragen zu blockieren, oder deaktivieren Sie die Option, um anonyme Internet-Anfragen zuzulassen.

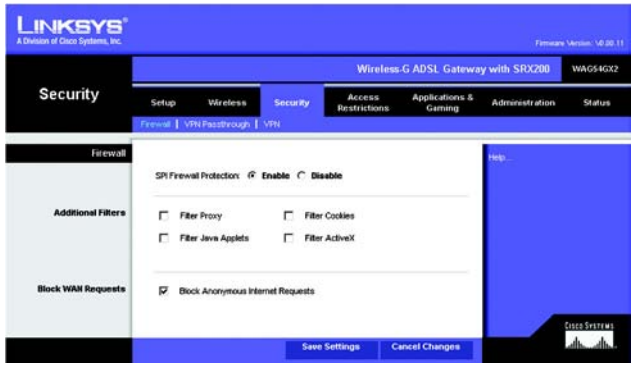


**Abbildung 6-25: Firewall**

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

## Registerkarte „VPN Passthrough“ (VPN-Passthrough)

VPN (*Virtual Private Networking*) ist eine Sicherheitsmaßnahme, durch die eine sichere Verbindung zwischen zwei entfernten Standorten hergestellt wird. Konfigurieren Sie die folgenden Einstellungen so, dass das Gateway die Übertragung durch VPN-Tunnel zulässt.

**Abbildung 6-26: „VPN Passthrough“ (VPN-Passthrough)**

### „VPN Passthrough“ (VPN-Passthrough)

- **IPSec Passthrough** (IPSec-Passthrough): IPSec (*Internet Protocol Security*) ist ein Protokollsatz, der zur Implementierung eines sicheren Paketaustauschs auf der IP-Ebene verwendet wird. Um IPSec-Passthrough zu aktivieren, klicken Sie auf das Optionsfeld **Enable** (Aktivieren). Um IPSec-Passthrough zu deaktivieren, klicken Sie auf das Optionsfeld **Disable** (Deaktivieren).

- **PPTP Passthrough** (PPTP-Passthrough): PPTP-Passthrough (*Point-to-Point Tunneling Protocol Passthrough*) ist eine Methode zur Aktivierung von VPN-Sitzungen auf einem Windows NT 4.0- oder Windows 2000-Server. Um PPTP-Passthrough zu aktivieren, klicken Sie auf das Optionsfeld **Enable** (Aktivieren). Um PPTP-Passthrough zu deaktivieren, klicken Sie auf das Optionsfeld **Disable** (Deaktivieren).

- **L2TP Passthrough** (L2TP-Passthrough): Bei L2TP-Passthrough (*Layering 2 Tunneling Protocol Passthrough*) handelt es sich um eine Erweiterung von PPTP (Point-to-Point Tunneling Protocol), mit der der Betrieb eines VPN über das Internet ermöglicht wird. Um P2TP-Passthrough zu aktivieren, klicken Sie auf die Optionsschaltfläche **Enable** (Aktivieren). Um P2TP-Passthrough zu deaktivieren, klicken Sie auf das Optionsfeld **Disable** (Deaktivieren).

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

## Registerkarte „VPN“

VPN (*Virtual Private Networking*) ist eine Sicherheitsmaßnahme, durch die eine sichere Verbindung zwischen zwei entfernten Standorten hergestellt wird. Mit diesen Einstellungen lassen Sie bis zu fünf VPN-Tunnel durch das Gateway anlegen.

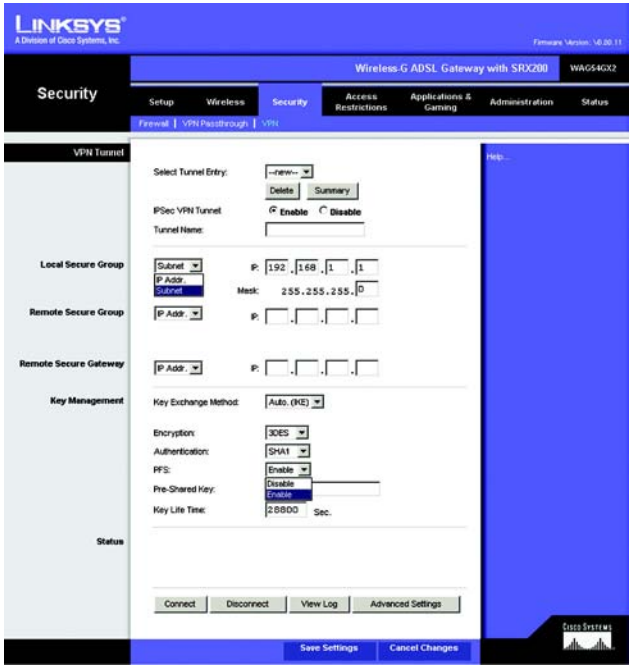


**Abbildung 6-27: VPN**

### „VPN Tunnel“ (VPN-Tunnel)

- **Select Tunnel Entry** (Tunneleintrag auswählen): Um diesen Tunnel einzurichten, wählen Sie **New** (Neu). Sollen die Einstellungen für einen Tunnel geändert werden, wählen Sie den gewünschten Tunnel aus.
- **Delete** (Löschen): Zum Löschen eines Tunnels wählen Sie diesen im Dropdown-Menü aus, und klicken Sie auf die Schaltfläche **Delete** (Löschen).
- **Summary** (Zusammenfassung): Um die Einstellungen für einen Tunnel abzurufen, wählen Sie den gewünschten Tunnel im Dropdown-Menü aus, und klicken Sie auf die Schaltfläche **Summary** (Zusammenfassung).
- **IPSec VPN Tunnel** (IPSec VPN-Tunnel): Soll der aktuelle VPN-Tunnel aktiviert werden, wählen Sie entsprechend **Enable** (Aktivieren). Andernfalls wählen Sie **Disable** (Deaktivieren) aus.
- **Tunnel Name** (Tunnelname): Wenn der Tunnel aktiviert ist, geben Sie den Namen des Tunnels ein. Verwenden Sie eindeutige Namen, um so mehrere Tunnel zweifelsfrei voneinander unterscheiden zu können. Der Name, den Sie dem Tunnel am lokalen Ende geben, muss nicht mit dem Namen am entfernten Ende des Tunnels übereinstimmen.

„Local Secure Group“ (Lokale sichere Gruppe)

Die lokale sichere Gruppe umfasst die Computer in Ihrem lokalen Netzwerk, die auf den Tunnel zugreifen können. Wählen Sie im Dropdown-Menü die Option **IP Addr.** (IP-Adresse) oder **Subnet** (Subnetz) aus.

- „IP Addr.“ (IP-Adr.) Mit der Option **IP Addr.** (IP-Adresse) können Sie einen bestimmten Computer angeben. Geben Sie anschließend in das Feld *IP* (IP-Adresse) die IP-Adresse des Computers ein.
- **Subnet** (Subnetz): Mit der Option **Subnet** (Subnetz) nehmen Sie das gesamte Netzwerk in den Tunnel auf. Geben Sie anschließend in das Feld *IP* (IP-Adresse) die IP-Adresse des Gateways ein und in das Feld *Mask* (Maske) entsprechend die Subnetzmaske.

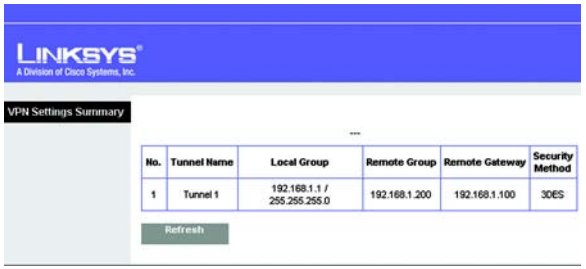


**Abbildung 6-28: „VPN Settings Summary“ (Zusammenfassung der VPN-Einstellungen)**

„Remote Secure Group“ (Entfernte sichere Gruppe)

Die entfernte sichere Gruppe umfasst die Computer am entfernten Ende des Tunnels, also die Computer, die auf den Tunnel zugreifen können. Wählen Sie im Dropdown-Menü die Option **IP Addr.** (IP-Adresse), **Subnet** (Subnetz) oder **Any** (Alle) aus.

- **IP Addr.** (IP-Adr.) Mit der Option **IP Addr.** (IP-Adresse) können Sie einen bestimmten Computer angeben. Geben Sie anschließend in das Feld *IP* (IP-Adresse) die IP-Adresse des Computers ein.
- **Subnet** (Subnetz): Mit der Option **Subnet** (Subnetz) nehmen Sie das gesamte Netzwerk in den Tunnel auf. Geben Sie in das Feld *IP* (IP-Adresse) die IP-Adresse des entfernten VPN-Geräts ein (z. B. für einen Router) und in das Feld *Mask* (Maske) die zugehörige Subnetzmaske.
- **Any** (Alle): Mit der Option **Any** (Alle) legen Sie fest, dass Anforderungen von jeglicher IP-Adresse durch das Gateway angenommen werden.

„Remote Secure Gateway“ (Entferntes Sicherheits-Gateway)

Das entfernte Sicherheits-Gateway ist das VPN-Gerät am entfernten Ende des VPN-Tunnels. Das VPN-Gerät kann ein VPN-Router, ein VPN-Server oder ein Computer mit VPN-Client-Software sein, der IPSec unterstützt. Wählen Sie im Dropdown-Menü die Option **IP Addr.** (IP-Adresse) oder **Any** (Alle) aus.

- **IP Addr.** (IP-Adr.) Mit der Option **IP Addr.** (IP-Adresse) legen Sie eine statische IP-Adresse fest. Geben Sie anschließend in das Feld *IP* (IP-Adresse) die IP-Adresse des VPN-Geräts ein.
- **Any** (Alle): Mit der Option **Any** (Alle) legen Sie fest, dass Anforderungen von jeglicher IP-Adresse durch das Gateway angenommen werden.

„Key Management“ (Schlüsselverwaltung)

- **Key Exchange Method** (Methode für den Schlüsselaustausch): Wählen Sie die Option **Auto (IKE)** oder **Manual** (Manuell) als Methode für den Schlüsselaustausch ausd. An beiden Enden eines VPN-Tunnels muss derselbe Modus für die Schlüsselverwaltung verwendet werden. Beide Methoden werden im Folgenden beschrieben. Sobald Sie eine Methode auswählen, ändert sich dieses Fenster, und die verfügbaren Einstellungen für die Methode werden eingeblendet.

  Auto (IKE)

  IKE (*Internet Key Exchange*) ist ein Protokoll für den Internet-Schlüsselaustausch, mit dem Schlüsselmaterial für eine Sicherheitsverknüpfung (*Security Association*, SA) ausgehandelt wird. Bei IKE wird der entfernte IDE-Peer mithilfe des vorläufigen gemeinsamen Schlüssels authentifiziert.

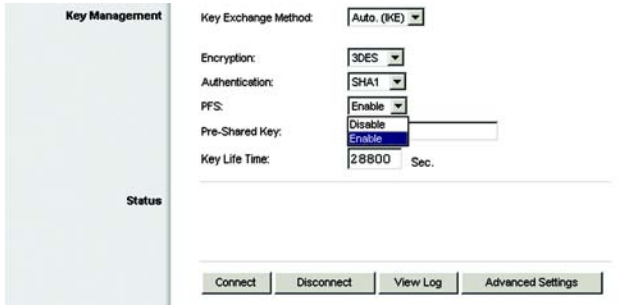


**Abbildung 6-29: „Key Exchange Method“ (Methode für den Schlüsselaustausch) – „Auto (IKE)“**

- **Encryption** (Verschlüsselung): Wenn Sie die Option **Auto (IKE)** auswählen, wird automatisch die 3DES-Verschlüsselung (168 Bit) aktiviert. Das VPN-Gerät am entfernten Ende des Tunnels muss dieselbe Verschlüsselungsart verwenden.

- **Authentication** (Authentifizierung): Wählen Sie eine der beiden verfügbaren Verschlüsselungsmethoden aus: **SHA1** oder **MD5**. MD5 besteht aus einem unidirektionalen Hash-Algorithmus, mit dem eine 128-Bit-Prüfsumme erzeugt wird. SHA ist ein unidirektionaler Hash-Algorithmus, der eine 160-Bit-Prüfsumme erzeugt. Die Verwendung von **SHA1** wird empfohlen, da diese Verschlüsselungsart sicherer ist. Stellen Sie sicher, dass an beiden Enden des VPN-Tunnels dieselbe Verschlüsselungsmethode eingesetzt wird.

- **PFS** (PFS, *Perfect Forward Secrecy*): PFS (*Perfect Forward Secrecy*) gewährleistet, dass der anfängliche Schlüsselaustausch und die IKE-Vorschläge sicher sind. Wählen Sie zum Verwenden von PFS die Option **Enable** (Aktivieren) aus. Andernfalls wählen Sie **Deaktivieren** aus.

- **Pre-Shared Key** (Vorläufiger gemeinsamer Schlüssel): Geben Sie eine Reihe von Zahlen oder Buchstaben in das Feld *Pre-shared Key* (Vorläufiger gemeinsamer Schlüssel) ein. Auf der Grundlage dieses Worts, das an beiden Enden des Tunnels eingegeben werden MUSS, wird ein Schlüssel erstellt, mit dem die über den Tunnel versendeten Daten verschlüsselt und entschlüsselt werden. Sie können in diesem Feld eine Kombination aus bis zu 24 Zahlen und Buchstaben eingeben. Es dürfen keine Sonderzeichen oder Leerzeichen verwendet werden.

- **Key Life Time** (Schlüssel-Verwendungsdauer): Hier können Sie die Gültigkeitsdauer eines Schlüssels festlegen. Geben Sie die gewünschte Nutzungszeit in Sekunden ein, oder lassen Sie das Feld leer, sodass der Schlüssel unbegrenzt lange zur Verfügung steht.

### „Manual“ (Manuell)

Bei der Option **Manual** (Manuell) erzeugen Sie den Schlüssel selbst; das Aushandeln eines Schlüssels ist nicht notwendig. Die manuelle Schlüsselverwaltung wird in der Regel in kleinen statischen Umgebungen sowie zur Fehlerbehebung eingesetzt.

- **Encryption Algorithm** (Verschlüsselungsalgorithmus): Wenn Sie die Option **Manual** (Manuell) auswählen, wird automatisch die 3DES-Verschlüsselung (168 Bit) aktiviert. Das VPN-Gerät am entfernten Ende des Tunnels muss dieselbe Verschlüsselungsart verwenden.

- **Encryption Key** (Verschlüsselungsschlüssel): Dieses Feld bestimmt den Schlüssel, der für die Ver- und Entschlüsselung des IP-Datenverkehrs eingesetzt werden soll. Der Verschlüsselungsschlüssel besteht aus 48 Bit; geben Sie also einen Schlüssel mit 24 ASCII-Zeichen ein. Stellen Sie sicher, dass an beiden Enden des VPN-Tunnels derselbe Verschlüsselungsschlüssel eingesetzt wird.

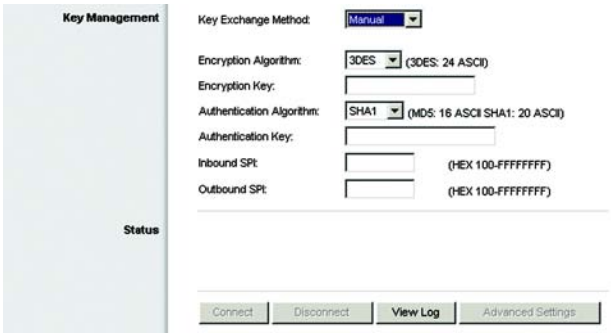


**Abbildung 6-30: „Key Exchange Method“ (Methode für den Schlüsselaustausch) – „Manual“ (Manuell)**

- **Authentication Algorithm** (Authentifizierungsalgorithmus): Wählen Sie eine Authentifizierungsmethode aus: **MD5** oder **SHA1**. Hiermit legen Sie das Verfahren fest, mit dem die ESP-Pakete authentifiziert werden. MD5 besteht aus einem unidirektionalen Hash-Algorithmus, mit dem eine 128-Bit-Prüfsumme erzeugt wird. SHA ist ein unidirektionaler Hash-Algorithmus, der eine 160-Bit-Prüfsumme erzeugt. Die Verwendung von **SHA1** wird empfohlen, da diese Verschlüsselungsart sicherer ist. Stellen Sie sicher, dass an beiden Enden des VPN-Tunnels dieselbe Verschlüsselungsmethode eingesetzt wird.

- **Authentication Key** (Authentifizierungsschlüssel): Dieses Feld bestimmt den Schlüssel, der für die Authentifizierung des IP-Datenverkehrs eingesetzt werden soll. Geben Sie einen Schlüssel mit Hexadezimalwerten ein. Bei der Option MD5 besteht der Authentifizierungsschlüssel aus 32 Bit; geben Sie daher 16 ASCII-Zeichen ein. Bei der Option SHA besteht der Authentifizierungsschlüssel aus 40 Bit, sodass entsprechend 20 ASCII-Zeichen einzugeben sind. Stellen Sie sicher, dass an beiden Enden des VPN-Tunnels derselbe Authentifizierungsschlüssel eingesetzt wird.

- **Inbound SPI** (Eingangs-SPI) und **Outbound SPI** (Ausgangs-SPI): Der SPI (*Security Parameter Index*, Sicherheitsparameter-Index) wird im ESP-Header (Encapsulating Security Payload) übertragen. Mit diesem Index sind der Empfänger und der Absender in der Lage, die Sicherheitsverknüpfung (*Security Association*, SA) auszuwählen, mit der ein Paket verarbeitet werden soll. Hexadezimalwerte sind möglich; der zulässige Bereich ist 100 bis ffffffff. Jeder Tunnel muss einen eindeutigen Eingangs-SPI und einen eindeutigen Ausgangs-SPI besitzen. Ein bestimmter SPI darf nicht von mehreren Tunneln verwendet werden. Der hier für **Inbound SPI** (Eingangs-SPI) eingestellte Wert muss dem Wert entsprechen, der am anderen Ende des Tunnels für eingestellt ist, und umgekehrt.

Status

Hier werden die Statusinformationen für die VPN-Tunnel des Gateways angezeigt.

Wenn Sie die Option **Manual** (Manuell) ausgewählt hatten, steht hier eine Schaltfläche bereit. Mit der Schaltfläche **View Log** (Protokoll anzeigen) rufen Sie die Aktivitätsprotokolle ab.

Wenn Sie die Option **Auto (IKE)** ausgewählt hatten, sind hier vier Schaltflächen verfügbar. Mit der Schaltfläche **Connect** (Verbinden) stellen Sie die VPN-Verbindung her.Mit der Schaltfläche **Disconnect** (Trennen) wird die VPN-Verbindung beendet. Mit der Schaltfläche **View Log** (Protokoll anzeigen) rufen Sie die Aktivitätsprotokolle ab. Mit der Schaltfläche **Advanced Settings** (Erweiterte Einstellungen) konfigurieren Sie die erweiterten Einstellungen für den VPN-Tunnel.

**Abbildung 6-31: „VPN Log“ (VPN-Protokoll)**

## „Advanced VPN Tunnel Setup“ (Erweiterte IPSec VPN-Tunnel-Einrichtung)

Klicken Sie auf die Schaltfläche **Advanced Settings** (Weitere Einstellungen). Das Fenster *Advanced VPN Tunnel Setup* (Erweiterte VPN-Tunnel-Einrichtung) wird geöffnet.

Diese erweiterten IPSec-Einstellungen sind fortgeschrittenen Benutzern vorbehalten.

### Phase 1

**Phase 1** wird zur Erstellung einer Sicherheitsverknüpfung (SA), auch „IKE SA“ (*Internet Key Exchange, Security Association*) genannt, verwendet. Nach Abschluss von Phase 1 wird in Phase 2 mindestens eine „IPSec SA“ erstellt und für IPSec-Sitzungen verwendet.

**Operation Mode** (Betriebsmodus): Die beiden verfügbaren Betriebsmodi **Main** (Hauptmodus) und **Aggressive** (Aggressiver Modus) tauschen die gleichen IKE-Nutzlasten auf unterschiedlichen Sequenzen aus. Der Hauptmodus wird häufiger verwendet, wobei einige Anwender jedoch den schnelleren aggressiven Modus vorziehen. Der Hauptmodus kann zur durchschnittlichen Verwendung eingesetzt werden und enthält mehr Authentifizierungserfordernisse als der aggressive Modus. Die Verwendung des Hauptmodus wird empfohlen, da dieser Modus sicherer ist. Bei beiden Modi werden vom VPN-Router Anfragen sowohl im Haupt- als auch im aggressiven Modus vom standortfernen VPN-Gerät akzeptiert.

**Local Identity** (Lokale Identität): Wählen Sie das Optionsfeld **Local IP address** (Lokale IP-Adresse) oder **Name** aus. Bei der Option **Local IP address** (Lokale IP-Adresse) wird die Internet-IP-Adresse des Gateways verwendet. Wenn Sie die Option **Name** auswählen, geben Sie den vollständigen Domänennamen (Fully Qualified Domain Name, FQDN) des Gateways in das entsprechende Feld ein, sodass dessen aktuelle IP-Adresse per DDNS aufgefunden werden kann.

**Remote Identity** (Entfernte Identität): Wählen Sie das Optionsfeld **Remote IP address** (Entfernte IP-Adresse) oder **Name** aus. Bei der Option **Remote IP address** (Entfernte IP-Adresse) wird die Internet-IP-Adresse des entfernten VPN-Geräts verwendet. Wenn Sie die Option **Name** auswählen, geben Sie den vollständigen Domänennamen (Fully Qualified Domain Name, FQDN) des entfernten VPN-Geräts in das entsprechende Feld ein, so dass dessen aktuelle IP-Adresse per DDNS aufgefunden werden kann.

**Encryption** (Verschlüsselung): Diese Option dient zur Ver- und Entschlüsselung von ESP-Paketen. Die 3DES-Verschlüsselung (168 Bit) wird automatisch aktiviert.

**Authentication** (Authentifizierung): Wählen Sie die Methode aus, die zur Authentifizierung von ESP-Paketen verwendet wird. Sie können zwischen zwei Methoden wählen: MD5 und SHA1. Die Verwendung von **SHA1** wird empfohlen, da diese Verschlüsselungsart sicherer ist.

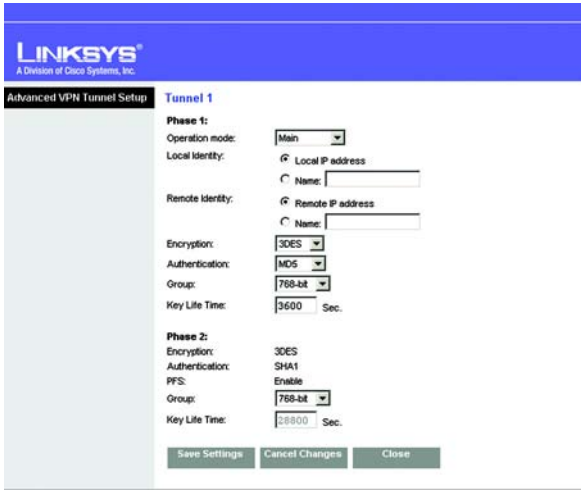


**Abbildung 6-32: „Advanced VPN Tunnel Setup“ (Erweiterte IPSec VPN-Tunnel-Einrichtung)**

**Group** (Gruppe): Es stehen drei Diffie-Hellman-Gruppen zur Auswahl: 768 Bit, 1024 Bit und 1536 Bit. Der Begriff Diffie-Hellman bezeichnet eine kryptografische Verschlüsselungstechnik, bei der sowohl öffentliche als auch private Schlüssel zur Ver- und Entschlüsselung verwendet werden.

**Key Life Time** (Schlüssel-Verwendungsdauer): Im Feld *Key Lifetime* (Schlüssel-Verwendungsdauer) können Sie die Gültigkeitsdauer eines Schlüssels festlegen. Geben Sie die gewünschte Nutzungszeit in Sekunden ein, sodass der Schlüssel bis zur erneuten Schlüsselverhandlung zwischen den Endpunkten zur Verfügung steht.

### Phase 2

**Encryption** (Verschlüsselung): Die in Phase 1 ausgewählte Verschlüsselungsmethode wird angezeigt.

**Authentication** (Authentifizierung): Die in Phase 2 ausgewählte Authentifizierungsmethode wird angezeigt.

**PFS**: Hier wird der Status der PFS-Funktion (Perfect Forward Secrecy) angezeigt.

**Group** (Gruppe): Es stehen drei Diffie-Hellman-Gruppen zur Auswahl: 768 Bit, 1024 Bit und 1536 Bit. Der Begriff Diffie-Hellman bezeichnet eine kryptografische Verschlüsselungstechnik, bei der sowohl öffentliche als auch private Schlüssel zur Ver- und Entschlüsselung verwendet werden.

**Key Life Time** (Schlüssel-Verwendungsdauer): Im Feld **Key Lifetime** (Schlüssel-Verwendungsdauer) können Sie die Gültigkeitsdauer eines Schlüssels festlegen. Geben Sie die gewünschte Nutzungszeit in Sekunden ein, sodass der Schlüssel bis zur erneuten Schlüsselverhandlung zwischen den Endpunkten zur Verfügung steht.

Klicken Sie nach dem Vornehmen aller Änderungen in diesem Fenster auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu speichern, oder klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen), um die Änderungen rückgängig zu machen.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

# Registerkarte „Access Restrictions“ (Zugriffsbeschränkungen)

## Registerkarte „Internet Access Policy“ (Richtlinien für Internetzugriff)

Im Fenster *Internet Access Policy* (Richtlinien für Internetzugriff) können Sie bestimmte Arten der Internetverwendung blockieren oder zulassen. Sie können für bestimmte Computer Richtlinien für den Internetzugriff einrichten und Websites nach URL-Adresse oder Schlüsselwort blockieren.

### „Internet Access Policy“ (Richtlinien für Internetzugriff)

**Internet Access Policy** (Richtlinien für Internetzugriff): Der Zugriff kann mithilfe einer Richtlinie verwaltet werden. Über die Einstellungen in diesem Fenster können Sie Zugriffsrichtlinien anwenden, nachdem Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern) geklickt haben. Wenn Sie im Dropdown-Menü eine Richtlinie auswählen, werden die Einstellungen dieser Richtlinie angezeigt. Wenn Sie eine Richtlinie löschen möchten, wählen Sie die Nummer dieser Richtlinie aus, und klicken Sie auf die Schaltfläche **Delete** (Löschen). Klicken Sie zum Anzeigen aller Richtlinien auf die Schaltfläche **Summary** (Zusammenfassung). (Sie können Richtlinien im Fenster *Summary* (Zusammenfassung) löschen, indem Sie die entsprechende Richtlinie auswählen und auf die Schaltfläche **Delete** (Löschen) klicken. Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum Fenster *Internet Access* (Internetzugriff) zurückzukehren.

**Status**: Die Richtlinien sind standardmäßig deaktiviert. Wenn Sie eine Richtlinie aktivieren möchten, wählen Sie im Dropdown-Menü die Nummer der Richtlinie aus, und klicken Sie auf die Optionsschaltfläche **Enable** (Aktivieren).

So erstellen Sie eine Richtlinie für den Internetzugriff:

1. Wählen Sie im Dropdown-Menü *Internet Access Policy* (Richtlinien für Internetzugriff) eine Nummer aus.
2. Klicken Sie auf die Optionsschaltfläche **Enable** (Aktivieren), um diese Richtlinie zu aktivieren.
3. Geben Sie in das vorgesehene Feld einen Richtliniennamen ein.

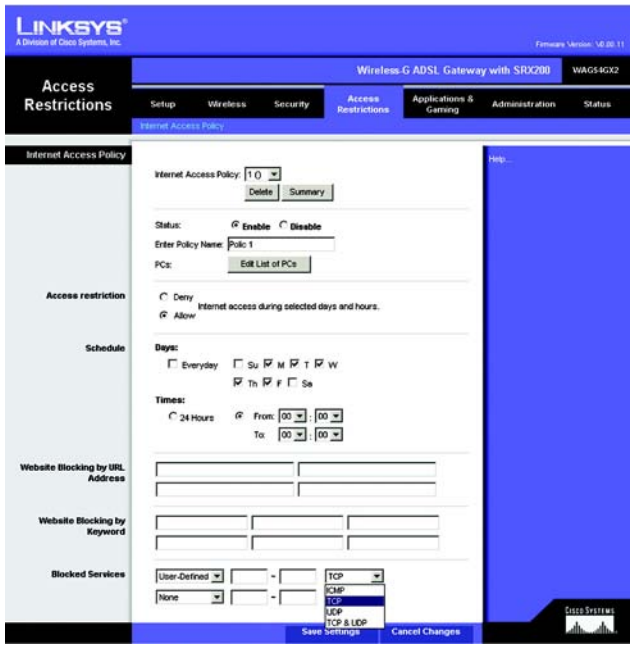


**Abbildung 6-33: „Internet Access Policy“ (Richtlinien für Internetzugriff)**

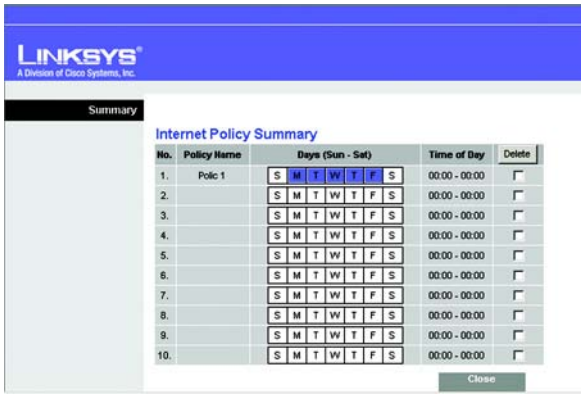


**Abbildung 6-34: „Internet Policy Summary“ (Internetrichtlinien – Zusammenfassung)**

4. Klicken Sie auf die Schaltfläche **Edit List of PCs** (PC-Liste bearbeiten), um die Computer auszuwählen, für die die Richtlinie gelten soll. Das Fenster *List of PCs* (PC-Liste) wird angezeigt. Ein PC kann nach MAC-Adresse oder IP-Adresse ausgewählt werden. Sie können auch eine Reihe von IP-Adressen eingeben, wenn die jeweilige Richtlinie für eine Gruppe von PCs gelten soll. Nachdem Sie die gewünschten Änderungen vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu übernehmen, oder auf **Cancel Changes** (Änderungen verwerfen), um die Änderungen zu verwerfen. Klicken Sie dann auf die Schaltfläche **Close** (Schließen), um das Fenster zu schließen.

5. Klicken Sie auf die entsprechende Option **Deny** (Verweigern) oder **Allow** (Zulassen), je nachdem, ob Sie den Internetzugriff für die im Fenster *List of PCs* (PC-Liste) aufgeführten Computer blockieren oder zulassen möchten.

6. Geben Sie an, an welchen Tagen und zu welchen Uhrzeiten diese Richtlinie gelten soll. Wählen Sie die einzelnen Tage aus, an denen die Richtlinie gültig sein soll, oder wählen Sie die Option **Everyday** (An allen Tagen) aus. Geben Sie anschließend den Gültigkeitszeitraum in Stunden und Minuten für die Richtlinie ein, oder wählen Sie die Option **24 Hours** (24 Stunden) aus.

7. Wenn Sie Websites mit bestimmten URL-Adressen blockieren möchten, geben Sie jeden URL in einem separaten Feld neben *Website Blocking by URL Address* (Website nach URL-Adresse blockieren) ein.

8. Wenn Sie Websites mithilfe bestimmter Schlüsselwörter blockieren möchten, geben Sie jedes Schlüsselwort in einem separaten Feld neben *Website Blocking by Keyword* (Website nach Schlüsselwort blockieren) ein.

9. Sie können den Zugang zu verschiedenen Diensten filtern, auf die über das Internet zugegriffen werden kann, z. B. FTP oder Telnet, indem Sie diese Dienste in den Dropdown-Menüs neben **Blocked Services** (Blockierte Dienste) auswählen. Die Port-Nummern und das Protokoll für den ausgewählten Dienst werden automatisch angezeigt.

   Wenn der gewünschte Dienst nicht aufgeführt ist, wählen Sie **User-Defined** (Benutzerdefiniert) aus. Geben Sie in den entsprechenden Feldern die Port-Nummern des Dienstes ein. Wählen Sie dann im Dropdown-Menü das Protokoll aus: **ICMP**, **TCP**, **UDP** oder **TCP & UDP**.

10. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Einstellungen der Richtlinie zu speichern. Um die Einstellungen der Richtlinie rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

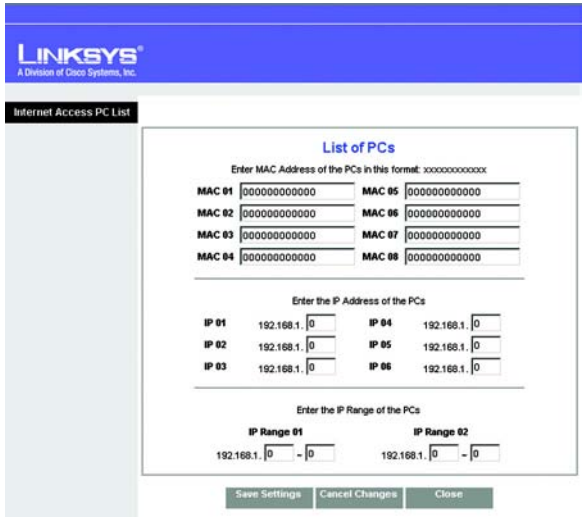


**Abbildung 6-35: „List of PCs“ (PC-Liste)**

# Registerkarte „Applications & Gaming“ (Anwendungen und Spiele)

## Registerkarte „Single Port Range Forwarding“ (Einfache Anschlussweiterleitung)

Verwenden Sie das Fenster *Single Port Range Forwarding* (Einfache Anschlussweiterleitung), wenn ein bestimmter Port geöffnet werden soll, damit Benutzer im Internet die Server hinter dem Gateway erkennen können (zu diesen Servern zählen u. a. FTP- oder E-Mail-Server). Wenn Anfragen dieser Art von Benutzern über das Internet an Ihr Netzwerk gesendet werden, leitet das Gateway diese Anfragen an den entsprechenden Computer weiter. Auf jedem Computer, dessen Anschluss weitergeleitet wird, muss die DCHP-Client-Funktion deaktiviert sein; darüber hinaus sollte jedem Computer eine neue statische IP-Adresse zugewiesen werden, da die IP-Adresse bei Verwendung der DHCP-Funktion u. U. geändert wird.

### „Single Port Forwarding“ (Einfache Anschlussweiterleitung)

- **Application** (Anwendung): Geben Sie den Namen der Anwendung im entsprechenden Feld ein.
- **External Port** (Externer Port) und **Internal Port** (Interner Port): Geben Sie die Nummern für den externen und internen Port ein.
- **Protocol** (Protokoll): Wählen Sie das Protokoll aus, das Sie für jede Anwendung verwenden möchten: **TCP** oder **UDP**.
- IP-Adresse: Geben Sie die IP-Adresse des entsprechenden Computers ein.
- **Enabled** (Aktiviert): Klicken Sie auf **Enabled** (Aktiviert), um die Weiterleitung für die ausgewählte Anwendung zu aktivieren.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

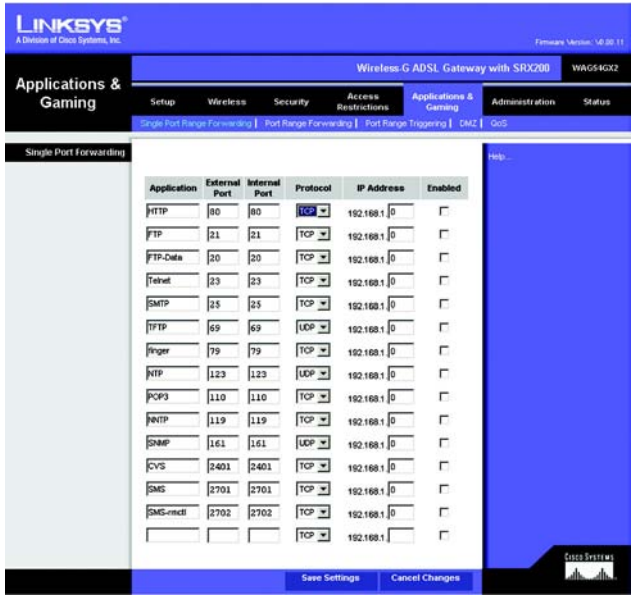


**Abbildung 6-36: „Single Port Forwarding“ (Einfache Anschlussweiterleitung)**

## Registerkarte „Port Range Forwarding“ (Weiterleitung an einen Anschlussbereich)

Im Fenster *Port Range Forwarding* (Weiterleitung an einen Anschlussbereich) können Sie öffentliche Dienste im Netzwerk festlegen, z. B. Web-, FTP-, E-Mail-Server oder andere spezielle Internetanwendungen. (Unter speziellen Internet-Anwendungen versteht man alle Anwendungen, die über den Internetzugang Funktionen wie z. B. Videokonferenzen oder Internet-Spiele ausführen. Bei einigen Internetanwendungen ist keine Weiterleitung erforderlich.)

Wenn Anfragen dieser Art von Benutzern über das Internet an Ihr Netzwerk gesendet werden, leitet das Gateway diese Anfragen an den entsprechenden Computer weiter. Auf jedem Computer, dessen Anschluss weitergeleitet wird, muss die DCHP-Client-Funktion deaktiviert sein; darüber hinaus sollte jedem Computer eine neue statische IP-Adresse zugewiesen werden, da die IP-Adresse bei Verwendung der DHCP-Funktion u. U. geändert wird.

### „Port Range Forwarding“ (Weiterleitung an einen Anschlussbereich)

- **Application** (Anwendung): Geben Sie den Namen der Anwendung im entsprechenden Feld ein.
- **Start** (Von) und **End** (Bis): Geben Sie die Anfangs- und Endnummern des Anschlussbereichs ein, der weitergeleitet werden soll.
- **Protocol** (Protokoll): Wählen Sie das Protokoll aus, das Sie für jede Anwendung verwenden möchten: **TCP**, **UDP** oder **Both** (Beide).
- „IP Address“ (IP-Adresse): Geben Sie die IP-Adresse des entsprechenden Computers ein.
- **Enable** (Aktivieren): Aktivieren Sie das Kontrollkästchen **Enable** (Aktivieren), um die Weiterleitung für die ausgewählte Anwendung zu aktivieren.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

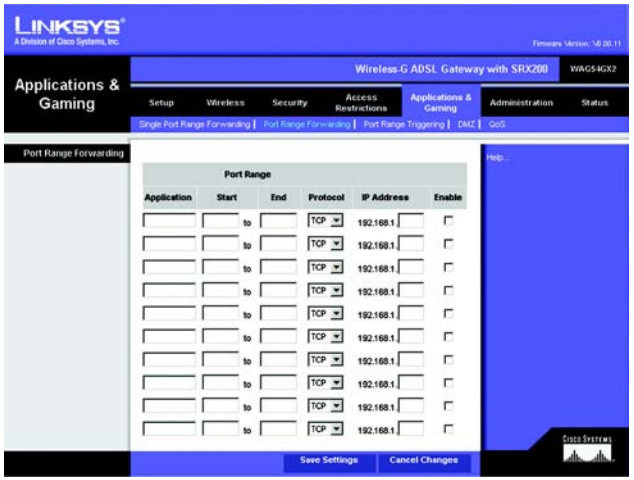


**Abbildung 6-37: „Port Range Forwarding“ (Weiterleitung an einen Anschlussbereich)**

## Registerkarte „Port Range Triggering“ (Anschlussbereich-Triggering)

Anschlussbereich-Triggering wird bei speziellen Anwendungen verwendet, über die ein Port auf Anfrage geöffnet werden kann. Bei dieser Funktion überprüft das Gateway ausgehende Daten auf spezielle Port-Nummern. Das Gateway speichert die IP-Adresse des Computers, der Daten zur Übertragung abruft. Wenn die abgerufenen Daten über das Gateway übertragen werden, werden die Daten über IP-Adresse und Port-Mapping-Regeln dem richtigen Computer weitergeleitet.

### „Port Range Triggering“ (Anschlussbereich-Triggering)

- **Application** (Anwendung): Geben Sie für jede Anwendung den gewünschten Namen ein.
- **Triggering Range** (Triggering-Bereich): Geben Sie die Anfangs- und Endnummern der Ports für den Triggering-Bereich ein.
- **Forwarded Range** (Weiterleitungsbereich): Geben Sie die Anfangs- und Endnummern der Ports für den Weiterleitungsbereich ein.
- **Enabled** (Aktiviert): Aktivieren Sie das Kontrollkästchen **Enabled** (Aktiviert), um das Anschlussbereich-Triggering für die ausgewählte Anwendung zu aktivieren.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

**Abbildung 6-38: „Port Rage Triggering“ (Anschlussbereich-Triggering)**

## Registerkarte „DMZ“

Über das Fenster *DMZ* kann mithilfe von DMZ-Hosting für einen lokalen Benutzer eine Verbindung zum Internet hergestellt werden, damit dieser spezielle Dienste (z. B. Internet-Spiele und Videokonferenzen) nutzen kann. Mit DMZ-Hosting werden alle Ports gleichzeitig an einen PC weitergeleitet, im Unterschied zu **Port Range Forwarding** (Weiterleitung an einen Anschlussbereich), bei dem nur maximal 10 Anschlussbereiche weitergeleitet werden können.

### DMZ

- **DMZ Hosting** (DMZ-Hosting): Mit der DMZ-Funktion (*Demilitarized Zone*, entmilitarisierte Zone) kann für einen lokalen Benutzer eine Verbindung zum Internet hergestellt werden, damit dieser spezielle Dienste (z. B. Internet-Spiele oder Videokonferenzen) nutzen kann.ann.ann. Klicken Sie auf **Enable** (Aktivieren), um diese Funktion zu verwenden. Klicken Sie auf **Disable** (Deaktivieren), um die DMZ-Funktion zu deaktivieren.

- **DMZ Host IP Address** (IP-Adresse des DMZ-Hosts): Um einen Computer mit dem Internet zu verbinden, geben Sie die IP-Adresse des Computers ein. Weitere Informationen zum Ermitteln der IP-Adresse eines Computers finden Sie in „Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters“.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

**Abbildung 6-39: DMZ**

## Registerkarte „QoS“

### QoS (Quality of Service)

QoS sorgt bei Netzwerkverkehr mit hoher Priorität, beispielsweise bei anspruchsvollen Echtzeitanwendungen wie Internettelefonie oder Videokonferenzen, für besseren Service.

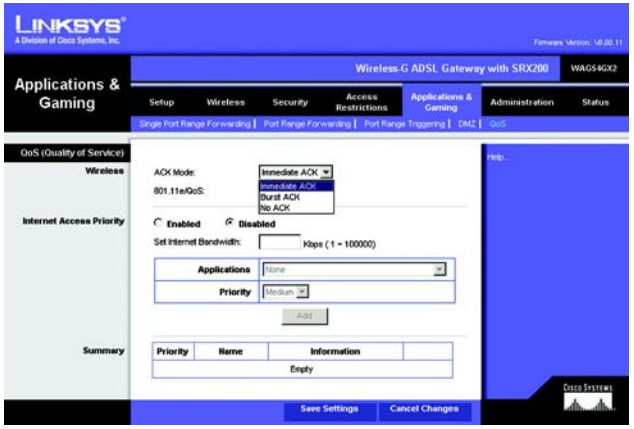


**Abbildung 6-40: QoS**

Wireless

- **ACK Mode** (ACK-Modus): Bei dieser Einstellung ist QoS für Benutzer priorisiert, bei denen auch der ACK-Modus aktiviert ist. Benutzer, bei denen die Option für das unmittelbare ACK-Signal aktiviert ist (Standardeinstellung), erzielen zuverlässige Verbindungen für die normale Nutzung des Netzwerks. Das diskontinuierliche ACK-Signal ist schneller, jedoch weniger zuverlässig, und kann sich negativ auf die Leistung im Wireless-Betrieb mit großer Reichweite auswirken. Die Einstellung **No ACK** (Kein ACK-Signal) deaktiviert die ACK-Funktion. Bei Clients mit ACK-Signal muss der Wireless-Adapter dieselbe Einstellung erhalten wie das Gateway. Dies ist in der Regel bei Multicast-Übertragungen wie Video der Fall. Diese Funktion sollten Sie nur als fortgeschrittener Benutzer verwenden.

- **802.11e/QoS**: QoS ist standardmäßig aktiviert, um so die bestmögliche Leistung für die Wireless-Verbindung zu erzielen. Bei einem gemischten Wireless-Netzwerk können Sie mit der Option **Disable** (Deaktivieren) die Leistungen noch verbessern.

**Internet Access Priority** (Priorität für Internetzugriff)

In diesem Bereich können Sie die Priorität auf Basis von Anwendung, Anschlussbereich oder MAC-Adresse festlegen. Es stehen vier Einstellungen für die Priorität zur Auswahl: **High** (Hoch), **Medium** (Mittel), **Normal** und **Low** (Niedrig).

- **Enable/Disable** (Aktivieren/Deaktivieren): Um die ausgehende Bandbreite für die verwendeten QoS-Richtlinien einzuschränken, wählen Sie die Option **Enabled** (Aktiviert) aus. Andernfalls wählen Sie **Disabled** (Deaktiviert) aus.

- **Set Internet Bandwidth** (Internetbandbreite einstellen): Mit dieser Einstellung können Sie die ausgehende Bandbreite für die verwendeten QoS-Richtlinien einschränken. Auf diese Weise können Sie steuern, wie viel Bandbreite eine bestimmte Anwendung verwenden darf. Geben Sie in dieses Feld die Bandbreite ein.

- **Application** (Anwendung): Hier stehen die Optionen **None** (Keine), **Online Game** (Online-Spiel), **MSN Messenger**, **YAHOO Messenger**, **Skype**, **Voice Device** (Sprachgerät) und **Add a New Application** (Neue Anwendung hinzufügen) zur Verfügung; außerdem können Sie aus einer Liste von Anwendungen auswählen. Um einen neuen Eintrag anzulegen, wählen Sie **Add a New Application** (Neue Anwendung hinzufügen), und beachten Sie den Bereich *Add a New Application* (Neue Anwendung hinzufügen).

- **Priority** (Priorität): Wählen Sie die Option **High** (Hoch), **Medium** (Mittel), **Normal** oder **Low** (Niedrig) für die Bandbreitenpriorität, die für die ausgewählte Anwendung erforderlich ist. Legen Sie nicht bei allen Anwendungen die Option **High** (Hoch) fest, weil hierdurch der Sinn und Zweck einer Zuweisung der verfügbaren Bandbreite aufgehoben würde. Soll die Bandbreite unter dem normalen Wert liegen, wählen Sie **Low** (Niedrig). Je nach Anwendung sind mehrere Versuche notwendig, um die passende Bandbreitenpriorität zu ermitteln. Klicken Sie abschließend auf **Add** (Hinzufügen), um den Eintrag in die Liste **Summary** (Zusammenfassung) aufzunehmen.

**Online Game** (Online-Spiel)

Mit der Option **Online Game** (Online-Spiel) öffnen Sie das Dropdown-Menü *Select a Game* (Spiel auswählen), in dem einige gängige, vorkonfigurierte Spiele aufgeführt sind. Wählen Sie das gewünschte Spiel in der Liste aus, und legen Sie die zugehörige Priorität fest.

MSN Messenger

Wählen Sie die Priorität in der Dropdown-Liste aus, und klicken Sie auf **Add** (Hinzufügen).

YAHOO Messenger

Wählen Sie die Priorität in der Dropdown-Liste aus, und klicken Sie auf **Add** (Hinzufügen).

Skype

Wählen Sie die Priorität in der Dropdown-Liste aus, und klicken Sie auf **Add** (Hinzufügen).

**Voice Device** (Sprachgerät)

Geben Sie in das Feld *Enter a Name* (Name eingeben) den Namen des Netzwerkgeräts ein, geben Sie die MAC-Adresse an, wählen Sie die Priorität in der Dropdown-Liste aus, und klicken Sie auf **Add** (Hinzufügen).

**Add a New Application** (Neue Anwendung hinzufügen)

**Enter a Name** (Name eingeben) — Geben Sie einen Namen für den Eintrag ein.

**Category** (Kategorie) — Wählen Sie die Option **Port Range** (Anschlussbereich) oder **MAC Address** (MAC-Adresse) für das Gateway, über das die Bandbreitenpriorität festgelegt werden soll.

**Port Range** (Anschlussbereich) — Wenn Sie die Option **Port Range** (Anschlussbereich) ausgewählt haben, steht diese Kategorie zur Verfügung. Hiermit können Sie den oder die Anschlussbereiche festlegen, die von der Anwendung genutzt werden sollen. Um beispielsweise die Bandbreite für FTP zuzuweisen, geben Sie **21-21** ein. Wenn Dienste für eine Anwendung benötigt werden, die auf Anschlüsse zwischen 1000 und 1250 zugreift, geben Sie entsprechend **1000-1250** ein. Zulässige Werte für die Anschlussnummern sind 1 bis 65535. Weitere Informationen zu den verwendeten Dienst-Ports finden Sie in der Dokumentation zur jeweiligen Anwendung.

**Abbildung 6-41: QoS – „Online Game“ (Online-Spiel)**

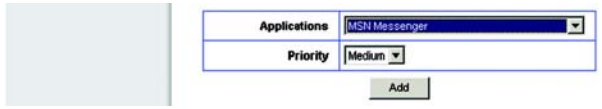


**Abbildung 6-42: QoS – MSN Messenger**

**Abbildung 6-43: QoS – „Voice Device“ (Sprachgerät)**

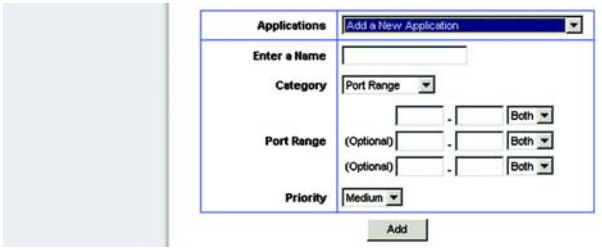


**Abbildung 6-44: QoS – „Add a New Application“ (Neue Anwendung hinzufügen) – „Port Range“ (Anschlussbereich)**

Sie können bis zu drei Bereiche für diese Bandbreitenzuweisung definieren. Legen Sie für die einzelnen Anschlussbereiche jeweils den oder die Protokolltyp(en) fest: **TCP**, **UDP** oder **Both** (Beide).

**MAC Address** (MAC-Adresse) Wenn Sie die Option **MAC Address** (MAC-Adresse) ausgewählt haben, steht diese Kategorie zur Verfügung. Geben Sie die zwölfstellige hexadezimale MAC-Adresse für das Gerät ein, das als Bandbreitenpriorität festgelegt werden soll. Diese Angabe bildet eine eindeutige ID für das Netzwerkgerät. Sobald das eingegebene Gerät im Gateway erkannt wird, erhält es die Priorität, die für den zugehörigen Eintrag eingestellt wurde. Weitere Informationen zum Abrufen der MAC-Adresse finden Sie in der Dokumentation zum Gerät.

**Priority** (Priorität) Legen Sie die Bandbreitenpriorität für die ausgewählte Anwendung fest. Für die Bandbreite stehen die Optionen **High** (Hoch), **Medium** (Mittel), **Normal** und **Low** (Niedrig) zur Auswahl; stellen Sie jedoch nicht alle Anwendungen auf **High** (Hoch) ein. Klicken Sie abschließend auf **Add** (Hinzufügen), um den Eintrag in die Liste **Summary** (Zusammenfassung) aufzunehmen.

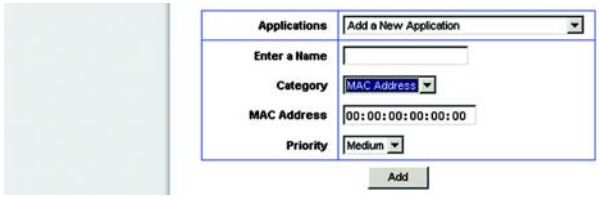


**Abbildung 6-45: QoS – „Add a New Application“ (Neue Anwendung hinzufügen) – „MAC Address“ (MAC-Adresse)**

## „Summary“ (Zusammenfassung)

**Priority** (Priorität) Hier wird die Priorität für die Bandbreitenzuweisung angezeigt, die Sie für die Anwendung festgelegt haben, und zwar **High** (Hoch), **Medium** (Mittel), **Normal** oder **Low** (Niedrig).

**Name** Hier wird der Name der Anwendung angezeigt (bzw. die Einträge), die für die Zuweisung angegeben wurde.

**Information** (Informationen) Hier wird der Anschlussbereich oder die MAC-Adresse angezeigt, die Sie beim Hinzufügen einer neuen Anwendung eingegeben haben. Bei vorkonfigurierten Anwendungen wird in diesem Bereich kein gültiger Eintrag aufgeführt.

**Remove** (Entfernen) Mit dieser Schaltfläche können Sie den Eintrag einer Anwendung entfernen. Soll der Eintrag gelöscht werden, klicken Sie auf die Schaltfläche **Remove** (Entfernen). Zum Speichern der Konfiguration klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern). Um Ihre Änderungen zu verwerfen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

# Registerkarte „Administration“ (Verwaltungsfunktionen)

## Registerkarte „Management“ (Verwaltungsfunktionen)

Über das Fenster *Management* (Verwaltungsfunktionen) können Sie die Einstellungen für den Gateway-Zugriff sowie die Verwaltungsfunktionen für SNMP (*Simple Network Management Protocol*), UPnP (*Universal Plug and Play*) und WLAN ändern.

### „Gateway Access“ (Gateway-Zugriff)

**Local Gateway Access** (Lokaler Gateway-Zugriff): Um die Sicherheit des Gateways zu gewährleisten, werden Sie beim Zugriff auf das webbasierte Dienstprogramm des Gateways zur Eingabe Ihres Passworts aufgefordert. Der Standardbenutzername und das Standardpasswort lauten **admin**.

- **Gateway Userlist** (Gateway-Benutzerliste): Wählen Sie die Nummer des Benutzers im Dropdown-Menü aus.
- **Gateway Username** (Gateway-Benutzername): Geben Sie den Standardbenutzernamen **admin** ein. Es wird empfohlen, dass Sie den Standardbenutzernamen in einen persönlichen Benutzernamen ändern.
- **Gateway Password** (Gateway-Passwort): Es empfiehlt sich, das Standardpasswort **admin** in ein Passwort Ihrer Wahl zu ändern.
- **Re-enter to confirm** (Zur Bestätigung erneut eingeben): Geben Sie das neue Gateway-Passwort erneut ein, um es zu bestätigen.

**Remote Gateway Access** (Remote-Gateway-Zugriff): Mit dieser Funktion können Sie auf das Gateway von einem entfernten Standort aus über das Internet zugreifen.

- **Remote Management** (Remote-Verwaltung): Mit dieser Funktion können Sie das Gateway von einem Remote-Standort über das Internet verwalten. Klicken Sie zum Aktivieren von **Remote Management** (Remote-Verwaltung) auf **Enable** (Aktivieren).

**WICHTIG:** Durch Aktivieren der Option **Remote Management** (Remote-Verwaltung) kann jeder Benutzer, der Ihr Passwort kennt, von jedem beliebigen Standort im Internet das Gateway konfigurieren.

- **Management Port** (Management-Port): Geben Sie die Anschlussnummer ein, die Sie für den entfernten Zugriff auf das Gateway verwenden möchten.

**Abbildung 6-46: „Management“ (Verwaltungsfunktionen)**

### SNMP

SNMP ist ein häufig verwendetes Protokoll zur Netzwerküberwachung und -verwaltung.

- **Device Name** (Gerätename): Geben Sie den Namen des Gateways ein.
- **SNMP**: Klicken Sie zur Verwendung von SNMP auf **Enable** (Aktivieren). Klicken Sie auf **Disabled** (Deaktiviert), um SNMP zu deaktivieren.
- **Get Community** (Get-Gemeinschaft): Geben Sie das Passwort ein, mit dem ein schreibgeschützter Zugriff auf die SNMP-Informationen des Gateways gewährt wird.
- **Set Community** (Set-Gemeinschaft): Geben Sie das Passwort ein, mit dem ein Schreib-/Lesezugriff auf die SNMP-Informationen des Gateways gewährt wird.
- **Trap Management: Trap to** (Trap-Verwaltung: Trap-Ziel): Geben Sie die IP-Adresse des entfernten Host-Computers ein, der die Trap-Nachrichten erhalten wird.

### UPnP

Mit UPnP kann das Gateway unter Windows ME und XP automatisch für verschiedene Internetanwendungen (z. B. Internet-Spiele oder Videokonferenzen) konfiguriert werden.

- **UPnP**: Klicken Sie zur Verwendung von UPnP auf **Enable** (Aktivieren). Klicken Sie andernfalls auf **Disable** (Deaktivieren).

### WLAN

- **Management via WLAN** (Verwaltung über WLAN): Mit dieser Funktion kann das Gateway über einen Wireless-Computer des lokalen Netzwerks verwaltet werden, wenn sich dieser beim webbasierten Dienstprogramm des Gateways anmeldet. Klicken Sie zum Aktivieren dieser Funktion auf **Enable** (Aktivieren). Klicken Sie andernfalls auf **Disable** (Deaktivieren).

### IGMP

- **IGMP Proxy** (IGMP-Proxy): Wenn die Multimediaanwendung oder das Gerät hinter dem Gateway nicht ordnungsgemäß funktioniert, können Sie mit der IGMP-Proxy-Funktion den Multicast-Datenverkehr durch das Gateway zulassen. Klicken Sie zur Verwendung dieser Funktion auf **Enable** (Aktivieren). Klicken Sie andernfalls auf **Disable** (Deaktivieren).

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

## Registerkarte „Reporting“ (Berichtaufzeichnung)

Im Fenster *Reporting* (Berichtaufzeichnung) wird ein Protokoll angezeigt, in dem alle eingehenden und ausgehenden URLs bzw. IP-Adressen für die Internetverbindung aufgeführt sind. Über diese Registerkarte stehen auch Protokolle für VPN- und Firewall-Ereignisse zur Verfügung.

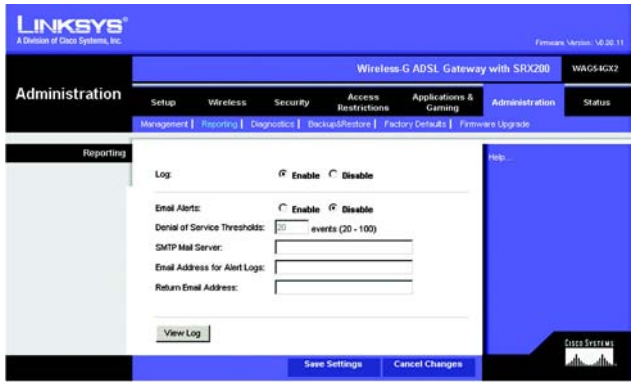


**Abbildung 6-48: „Reporting“ (Berichtaufzeichnung)**

### „Reporting“ (Berichtaufzeichnung)

- **Log** (Protokoll): Klicken Sie zur Verwendung der Berichtaufzeichnung auf **Enable** (Aktivieren).

### „Email Alerts“ (E-Mail-Warnungen)

- **Email Alerts** (E-Mail-Warnungen): Klicken Sie auf die Option **Enable** (Aktivieren), um E-Mail-Warnungen zu verwenden.
- **Denial of Service Thresholds** (DoS-Schwellwerte): Geben Sie die Anzahl der DoS-Angriffe (*Denial of Service*) ein, durch die eine E-Mail-Warnung ausgelöst werden soll.
- **SMTP Mail Server** (SMTP-Mailserver): Geben Sie die IP-Adresse des SMTP-Servers ein.
- **E-Mail Address for Alert Logs** (E-Mail-Adresse für Warnungsprotokolle): Geben Sie die E-Mail-Adresse ein, an die Warnungsprotokolle gesendet werden sollen.
- **Return E-Mail address** (E-Mail-Antwortadresse): Geben Sie die Antwortadresse für die E-Mail-Warnungen ein.

Wenn Sie die Protokolle anzeigen möchten, klicken Sie auf die Schaltfläche **View Logs** (Protokolle anzeigen). Es wird ein neues Fenster angezeigt. Wählen Sie im Dropdown-Menü das anzuzeigende Protokoll aus: **ALL** (ALLE), **Access Log** (Zugriffsprotokoll) oder **Firewall Log** (Firewall-Protokoll). Klicken Sie auf die Schaltfläche **pageRefresh** (Seite aktualisieren), um die Informationen zu aktualisieren. Klicken Sie auf die Schaltfläche **Clear** (Löschen), um die Protokollinformationen zu löschen. Klicken Sie auf die Schaltfläche **Previous Page** (Vorherige Seite), um zur vorherigen Informationsseite zu wechseln. Klicken Sie auf die Schaltfläche **Next Page** (Nächste Seite), um zur nächsten Informationsseite zu wechseln.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

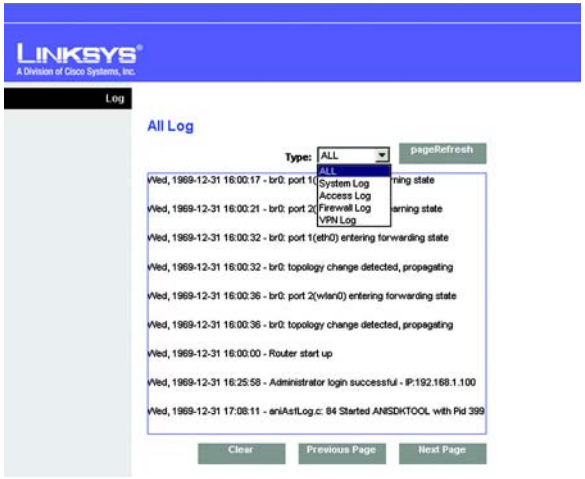


**Abbildung 6-49: „System Log“ (Systemprotokoll)**

## Registerkarte „Diagnostics“ (Diagnose)

In diesem Fenster können Sie Ping-Tests durchführen und die Testergebnisse anzeigen.

### „Ping Test“ (Ping-Test)

**Ping Test Parameters** (Ping-Test-Parameter)

- **Ping Target IP** (Ping-Ziel-IP-Adresse): Geben Sie die IP-Adresse ein, für die Pings durchgeführt werden sollen. Dies kann eine lokale IP-Adresse (LAN) oder eine Internet-IP-Adresse (WAN) sein.
- **Ping Size** (Ping-Größe): Geben Sie die Größe des Pakets an.
- **Number of Pings** (Anzahl der Pings): Geben Sie die Anzahl der Pings an, die durchgeführt werden soll.
- **Ping Interval** (Ping-Intervall): Geben Sie das Ping-Intervall (wie oft Pings für die Ziel-IP-Adresse durchgeführt werden sollen) in Millisekunden ein.
- **Ping Timeout** (Ping-Wartezeit): Geben Sie die Ping-Wartezeit (Zeitraum, nach dem der Ping-Test abläuft) in Millisekunden ein.

Klicken Sie auf die Schaltfläche **Start Test** (Test starten), um den Ping-Test zu starten.

- **Ping Result** (Ping-Ergebnisse): In dieser Zeile werden die Ergebnisse des Ping-Tests angezeigt.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

**Abbildung 6-50: „Diagnostics“ (Diagnose)**

## Registerkarte „Backup & Restore“ (Sichern & Wiederherstellen)

Auf der Registerkarte **Backup & Restore** (Sichern & Wiederherstellen) können Sie eine Sicherungskopie der Konfigurationsdatei des Gateways erstellen und diese wiederherstellen.

### „Backup Configuration“ (Konfiguration sichern)

Klicken Sie zum Erstellen einer Sicherungskopie der Konfigurationsdatei des Gateways auf die Schaltfläche **Backup** (Sichern). Befolgen Sie dann die Anweisungen auf dem Bildschirm.

**Abbildung 6-51: „Backup&Restore“ (Sichern & Wiederherstellen)**

### „Restore Configuration“ (Konfiguration wiederherstellen)

Klicken Sie zum Wiederherstellen der Konfigurationsdatei des Gateways auf die Schaltfläche **Browse** (Durchsuchen). Befolgen Sie dann die Anweisungen auf dem Bildschirm, um nach der Datei zu suchen. Klicken Sie nach Auswahl der Datei auf die Schaltfläche **Restore** (Wiederherstellen).

Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

## Registerkarte „Factory Defaults“ (Werkseinstellungen)

In diesem Fenster können Sie die Werkseinstellungen des Gateways wiederherstellen.

### „Factory Defaults“ (Werkseinstellungen)

**Restore Factory Defaults** (Werkseinstellungen wiederherstellen): Wenn Sie das Gateway auf die Werkseinstellungen zurücksetzen möchten (Ihre Einstellungen gehen dabei verloren), klicken Sie auf **Restore Factory Defaults** (Werkseinstellungen wiederherstellen). Befolgen Sie dann die Anweisungen auf dem Bildschirm. Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

**Abbildung 6-52: „Factory Defaults“ (Werkseinstellungen)**

## Registerkarte „Firmware Upgrade“ (Aktualisieren der Firmware)

In diesem Fenster können Sie die Firmware des Gateways aktualisieren.

### „Firmware Upgrade“ (Aktualisieren der Firmware)

So aktualisieren Sie die Gateway-Firmware:

1. Laden Sie die Aktualisierungsdatei für die Gateway-Firmware unter www.linksys.com/international herunter.
2. Extrahieren Sie die Datei auf dem Computer.
3. Klicken Sie im Fenster *Firmware Upgrade* (Firmware aktualisieren) auf die Schaltfläche **Browse** (Durchsuchen), um die Firmware-Aktualisierungsdatei zu suchen.
4. Doppelklicken Sie auf die Firmware-Datei, die Sie heruntergeladen und extrahiert haben.
5. Klicken Sie auf die Schaltfläche **Start to Upgrade** (Aktualisierung starten), und befolgen Sie die Anweisungen auf dem Bildschirm.

Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

**Abbildung 6-53: „Firmware Upgrade“ (Aktualisieren der Firmware)**

# Registerkarte „Status“

## Registerkarte „Gateway“

In diesem Fenster werden Informationen zum Gateway und zur entsprechenden Internetverbindung angezeigt.

### „Gateway Information“ (Gateway-Informationen)

In diesem Bereich wird die Version der Gateway-Firmware, die MAC-Adresse und die aktuelle Uhrzeit angezeigt.

### „Internet Connection“ (Internetverbindung)

In diesem Bereich werden folgende Informationen angezeigt: **Login Type** (Anmeldetyp), **Interface** (Schnittstelle), **IP Address** (IP-Adresse), **Subnet Mask** (Subnetzmaske), **Default Gateway** (Standard-Gateway) und die IP-Adressen für die DNS-Server 1 bis 3.

**Abbildung 6-54: Gateway**

**DHCP Renew** (DHCP erneuern): Klicken Sie auf die Schaltfläche **DHCP Renew** (DHCP erneuern), sofern diese angezeigt wird, um die aktuelle IP-Adresse des Gateways durch eine neue IP-Adresse zu ersetzen.

**DHCP Release** (DHCP löschen): Klicken Sie auf die Schaltfläche **DHCP Release** (DHCP löschen), sofern diese angezeigt wird, um die aktuelle IP-Adresse des Gateways zu löschen.

Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren. Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

## Registerkarte „Local Network“ (Lokales Netzwerk)

In diesem Fenster werden Informationen zum lokalen Netzwerk des Gateways angezeigt.

### „Local Network“ (Lokales Netzwerk)

In diesem Fenster wird Folgendes angezeigt: die lokale MAC-Adresse, die IP-Adresse, die Subnetzmaske, der DHCP-Server sowie die erste und die letzte IP-Adresse.

Klicken Sie zum Anzeigen der DHCP-Client-Tabelle auf die Schaltfläche **DHCP Client Table** (DHCP-Client-Tabelle). Klicken Sie zum Anzeigen der ARP/RARP-Tabelle auf die Schaltfläche **ARP/RARP Table** (ARP/RARP-Tabelle).

**DHCP Client Table** (DHCP-Client-Tabelle): Im Bereich **DHCP Active IP Table** (DHCP – Tabelle zur aktiven IP-Adresse) werden die aktuellen DHCP-Client-Daten angezeigt. Zu diesen Angaben zählen der Computername, die IP-Adresse, die MAC-Adresse und der Zeitpunkt, zu dem die dynamische IP-Adresse für Clients abläuft, die den DHCP-Server verwenden. (Diese Daten werden im temporären Speicher gespeichert und ändern sich in regelmäßigen Abständen.) Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren. Um einen Client vom DHCP-Server zu löschen, wählen Sie den entsprechenden Client aus, und klicken Sie anschließend auf die Schaltfläche **Delete** (Löschen). Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum Fenster *Local Network* (Lokales Netzwerk) zurückzukehren.

**ARP/RARP Table** (ARP/RARP-Tabelle): Bei einer ARP-Anfrage handelt es sich um eine Anfrage, mit der das Gateway die MAC-Adressen von Clients mit IP-Adressen anfragt, um IP-Adressen den entsprechenden MAC-Adressen zuordnen zu können. Bei RARP geht der Vorgang im Vergleich zu ARP umgekehrt vonstatten. Die ARP/RARP-Tabelle enthält die aktuellen Daten für das lokale Netzwerk des Gateways. Es werden die entsprechenden IP-Adressen und MAC-Adressen aufgeführt. (Diese Daten werden im temporären Speicher gespeichert und ändern sich in regelmäßigen Abständen.) Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren. Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum Fenster *Local Network* (Lokales Netzwerk) zurückzukehren.

Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren. Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

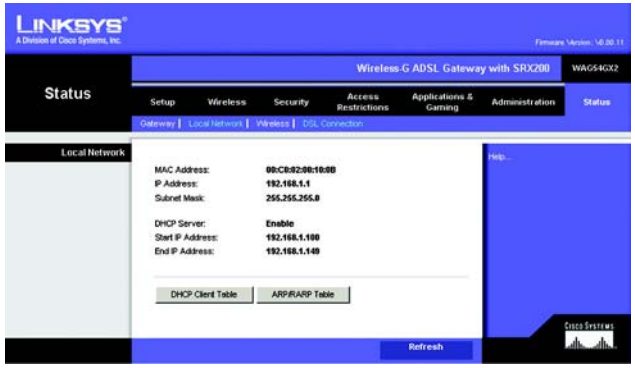


**Abbildung 6-55: „Local Network“ Lokales Netzwerk**

**Abbildung 6-56: DHCP – „DHCP Active IP Table“ (Tabelle zur aktiven IP-Adresse)**

**Abbildung 6-57: „ARP/RARP Table“ (ARP/RARP-Tabelle)**

## Registerkarte „Wireless“

In diesem Fenster werden Informationen zum Wireless-Netzwerk des Gateways angezeigt.

### Wireless

Dieses Fenster enthält folgende Angaben: die Versionsnummer der Wireless-Firmware, die MAC-Adresse, den Modus, die SSID, den Kanal und die Verschlüsselungsoption.

Klicken Sie auf die Schaltfläche **Wireless Clients Connected** (Angeschlossene Wireless-Clients), um eine Liste der Wireless-Clients anzuzeigen, die an das Gateway angeschlossen sind. Gleichzeitig werden die entsprechenden Computernamen, IP-Adressen und MAC-Adressen angezeigt. Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren. Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum Fenster *Wireless* zurückzukehren.

Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren. Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

**Abbildung 6-58: Wireless**

**Abbildung 6-59: „Networked Computers“ (Netzwerk-Computer)**

## Registerkarte „DSL Connection“ (DSL-Verbindung)

In diesem Fenster sind Informationen zur DSL-Verbindung aufgeführt.

### „DSL Status“ (DSL-Status)

Dieser Bereich enthält folgende Angaben: Status sowie Downstream- und Upstream-Rate.

### „PVC Connection“ (PVC-Verbindung)

In diesem Bereich werden folgende Informationen angezeigt: **Encapsulation** (Kapselungstyp), **Multiplexing**, **QoS**, **Pcr Rate** (PCR-Rate), **Scr Rate** (SCR-Rate), **Autodetect** (automatische Erkennung), **VPI**, **VCI**, **Enable Status** (Aktivierungsstatus) und **PVC Status** (PVC-Status).

Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren. Klicken Sie auf **Help** (Hilfe), um weitere Informationen zu erhalten.

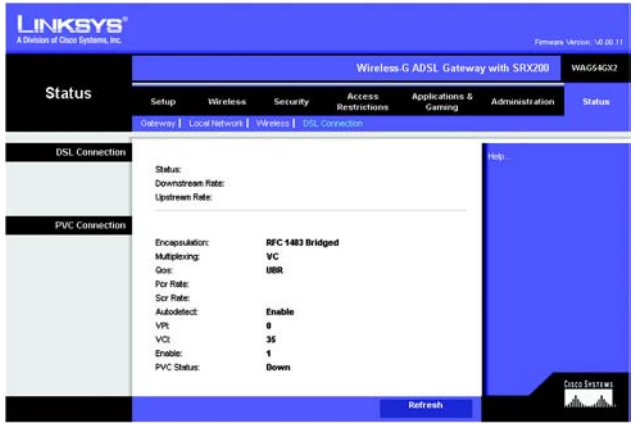


**Abbildung 6-60: „DSL Connection“ (DSL-Verbindung)**

# Anhang A: Fehlerbehebung

Dieser Anhang besteht aus zwei Teilen: „Behebung häufig auftretender Probleme“ und „Häufig gestellte Fragen“. Er enthält Lösungsvorschläge zu Problemen, die während der Installation und des Betriebs des Gateways auftreten können. Lesen Sie sich zur Fehlerbehebung die unten aufgeführten Beschreibungen durch. Wenn hier kein Lösungsvorschlag zu Ihrem Problem aufgeführt ist, finden Sie weitere Informationen auf der Website von Linksys unter www.linksys.com/international.

## Behebung häufig auftretender Probleme

1. ***Wie lege ich eine statische IP-Adresse auf einem Computer fest?***
   Führen Sie die folgenden Schritte aus, um einem Computer eine statische IP-Adresse zuzuweisen:
   - Für Benutzer von Windows 98 und ME:
     1. Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf die Option **Netzwerk**.
     2. Wählen Sie im Feld *Die folgenden Netzwerkkomponenten sind installiert* die mit dem Ethernet-Adapter verbundene Option **TCP/IP->** aus. Falls nur ein Ethernet-Adapter installiert ist, wird nur in einer Zeile **TCP/IP** ohne Verknüpfung mit einem Ethernet-Adapter aufgeführt. Wählen Sie den Eintrag aus, und klicken Sie auf die Schaltfläche **Eigenschaften**.
     3. Wählen Sie im Fenster für die TCP/IP-Eigenschaften auf der Registerkarte **IP-Adresse** die Option **IP-Adresse festlegen** aus. Geben Sie eine eindeutige IP-Adresse ein, die von keinem anderen an das Gateway angeschlossenen Computer im Netzwerk verwendet wird. Vergewissern Sie sich, dass für jeden Computer bzw. jedes Netzwerkgerät eine eindeutige IP-Adresse verwendet wird.
     4. Klicken Sie auf die Registerkarte **Gateway**, und geben Sie **192.168.1.1** ein, wenn die Eingabeaufforderung für das neue Gateway angezeigt wird (dies ist die Standard-IP-Adresse für das Gateway). Klicken Sie auf die Schaltfläche **Hinzufügen**, um die Eingabe zu übernehmen.
     5. Klicken Sie auf die Registerkarte **DNS**, und stellen Sie sicher, dass DNS aktiviert ist. Geben Sie den Host- und den Domänenname ein (z. B. „Johann“ als Hostname und „home“ als Domänenname). Geben Sie den DNS-Eintrag ein, den Sie von Ihrem ISP erhalten haben. Falls Sie keine DNS-IP-Adresse von Ihrem ISP erhalten haben, wenden Sie sich an Ihren ISP bzw. sehen Sie auf dessen Website nach, um diese Informationen zu erhalten.
     6. Klicken Sie im Fenster für die TCP/IP-Eigenschaften auf **OK**, und klicken Sie anschließend auf die Schaltfläche **Schließen** bzw. die Schaltfläche **OK**, um das Fenster **Netzwerk** zu schließen.
     7. Wenn Sie dazu aufgefordert werden, starten Sie den Computer neu.
   - Für Benutzer von Windows 2000:
     1. Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf **Netzwerk- und DFÜ-Verbindungen**.

2. Klicken Sie mit der rechten Maustaste auf die LAN-Verbindung, die mit dem von Ihnen verwendeten Ethernet-Adapter verknüpft ist, und wählen Sie die Option **Eigenschaften** aus.
3. Wählen Sie im Feld *Aktivierte Komponenten werden von dieser Verbindung verwendet* die Option **Internetprotokoll (TCP/IP)** aus, und klicken Sie auf die Schaltfläche **Eigenschaften**. Wählen Sie die Option **Folgende IP-Adresse verwenden** aus.
4. Geben Sie eine eindeutige IP-Adresse ein, die von keinem anderen an das Gateway angeschlossenen Computer im Netzwerk verwendet wird.
5. Geben Sie für die Subnetzmaske den Eintrag **255.255.255.0** ein.
6. Geben Sie für das Standard-Gateway den Eintrag **192.168.1.1** ein (die Standard-IP-Adresse des Gateways).
7. Wählen Sie im unteren Fensterbereich die Option **Folgende DNS-Serveradressen verwenden** aus, und geben Sie den bevorzugten und den alternativen DNS-Server ein (diese Angaben erhalten Sie von Ihrem ISP). Wenden Sie sich an Ihren ISP bzw. sehen Sie auf dessen Website nach, um diese Informationen zu erhalten.
8. Klicken Sie im Fenster *Internetprotokolleigenschaften (TCP/IP)* auf die Schaltfläche **OK** sowie im Fenster *Eigenschaften von LAN-Verbindung* auf die Schaltfläche **OK**.
9. Wenn Sie dazu aufgefordert werden, starten Sie den Computer neu.

- Für Benutzer von Windows XP:
  Die folgenden Anweisungen gelten, wenn Sie Windows XP mit der Standard-Benutzeroberfläche ausführen. Wenn Sie die klassische Benutzeroberfläche verwenden (bei der die Symbole und Menüs wie in vorherigen Windows-Versionen aussehen), befolgen Sie die Anweisungen für Windows 2000.
  1. Klicken Sie auf **Start** und **Systemsteuerung**.
  2. Klicken Sie auf das Symbol **Netzwerk- und Internetverbindungen** und dann auf **Netzwerkverbindungen**.
  3. Klicken Sie mit der rechten Maustaste auf die LAN-Verbindung, die mit dem von Ihnen verwendeten Ethernet-Adapter verknüpft ist, und wählen Sie die Option **Eigenschaften** aus.
  4. Wählen Sie im Feld *Diese Verbindung verwendet folgende Elemente* die Option **Internetprotokoll (TCP/IP)** aus. Klicken Sie auf die Schaltfläche **Eigenschaften**.
  5. Geben Sie eine eindeutige IP-Adresse ein, die von keinem anderen an das Gateway angeschlossenen Computer im Netzwerk verwendet wird.
  6. Geben Sie für die Subnetzmaske den Eintrag **255.255.255.0** ein.
  7. Geben Sie für das Standard-Gateway den Eintrag **192.168.1.1** ein (die Standard-IP-Adresse des Gateways).
  8. Wählen Sie im unteren Fensterbereich die Option **Folgende DNS-Serveradressen verwenden** aus, und geben Sie den bevorzugten und den alternativen DNS-Server ein (diese Angaben erhalten Sie von Ihrem ISP). Wenden Sie sich an Ihren ISP bzw. sehen Sie auf dessen Website nach, um diese Informationen zu erhalten.
  9. Klicken Sie im Fenster *Internetprotokolleigenschaften (TCP/IP)* auf die Schaltfläche **OK**. Klicken Sie im Fenster *Eigenschaften von LAN-Verbindung* auf die Schaltfläche **OK**.

***2. Ich möchte meine Internetverbindung prüfen.***

A. Überprüfen Sie Ihre TCP/IP-Einstellungen.

Für Benutzer von Windows 98, ME, 2000 und XP:

- Weitere Informationen finden Sie in der Windows-Hilfe. Stellen Sie sicher, dass in den Einstellungen die Option **IP-Adresse automatisch beziehen** aktiviert ist.

Für Benutzer von Windows NT 4.0:

- Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf das Symbol **Netzwerk**.
- Klicken Sie auf die Registerkarte **Protokoll**, und doppelklicken Sie auf **TCP/IP-Protokoll**.
- Wenn das Fenster angezeigt wird, stellen Sie sicher, dass Sie den richtigen Adapter als Ihren Ethernet-Adapter und die Option **IP-Adresse von einem DHCP-Server beziehen** ausgewählt haben.
- Klicken Sie im Fenster mit den TCP/IP-Protokolleigenschaften auf die Schaltfläche **OK** und im Fenster **Netzwerk** auf die Schaltfläche **Schließen**.
- Wenn Sie dazu aufgefordert werden, starten Sie den Computer neu.

B. Öffnen Sie eine Eingabeaufforderung.

Für Benutzer von Windows 98 und ME:

- Klicken Sie auf **Start** und **Ausführen**. Geben Sie im Feld *Öffnen* die Zeichenfolge **command** ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**.

Für Benutzer von Windows NT, 2000 und XP:

- Klicken Sie auf **Start** und **Ausführen**. Geben Sie im Feld *Öffnen* den Eintrag **cmd** ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**. Geben Sie an der Eingabeaufforderung die Zeichenfolge **ping 192.168.1.1** ein, und drücken Sie die Eingabetaste.
- Wenn Sie eine Antwort erhalten, kommuniziert der Computer mit dem Gateway.
- Wenn Sie KEINE Antwort erhalten, überprüfen Sie die Kabelverbindung, und stellen Sie sicher, dass in den TCP/IP-Einstellungen für den Ethernet-Adapter die Option **IP-Adresse automatisch beziehen** aktiviert ist.

C. Geben Sie an der Eingabeaufforderung die Zeichenfolge **ping** gefolgt von Ihrer Internet- bzw. WAN-IP-Adresse ein, und drücken Sie die Eingabetaste. Die Internet- bzw. WAN-IP-Adresse wird im Statusfenster des webbasierten Dienstprogramms des Gateways angezeigt. Beispiel: Wenn Ihre Internet- bzw. WAN-IP-Adresse 1.2.3.4 lautet, müssen Sie die Zeichenfolge **ping 1.2.3.4** eingeben und anschließend die Eingabetaste drücken.

- Wenn Sie eine Antwort erhalten, ist der Computer mit dem Gateway verbunden.
- Wenn Sie KEINE Antwort erhalten, geben Sie den Ping-Befehl an einem anderen Computer ein, um so sicherzustellen, dass das Problem nicht vom ersten Computer verursacht wird.

D. Geben Sie an der Eingabeaufforderung die Zeichenfolge **ping www.yahoo.com** ein, und drücken Sie die Eingabetaste.

- Wenn Sie eine Antwort erhalten, ist der Computer mit dem Internet verbunden. Wenn Sie KEINE Webseite öffnen können, geben Sie den Ping-Befehl an einem anderen Computer ein, um dadurch sicherzustellen, dass das Problem nicht vom ersten Computer verursacht wird.

- Wenn Sie KEINE Antwort erhalten, kann ein Verbindungsproblem vorliegen. Geben Sie den Ping-Befehl an einem anderen Computer ein, um dadurch sicherzustellen, dass das Problem nicht vom ersten Computer verursacht wird.

***3. Mit meiner Internetverbindung erhalte ich keine IP-Adresse im Internet.***

- Lesen Sie sich den oben aufgeführten Abschnitt „2. Ich möchte meine Internetverbindung prüfen“ durch, und überprüfen Sie anhand dessen Ihre Verbindung.
  1. Stellen Sie sicher, dass Sie die korrekten Einstellungen für die Internetverbindung verwenden. Wenden Sie sich an Ihren ISP, um die Art Ihrer Internetverbindung zu überprüfen: **RFC 1483 Bridged** (RFC 1483-Überbrückung), **RFC 1483 Routed** (RFC 1483-Weiterleitung), **RFC 2516 PPPoE**, **RFC 2364 PPPoA**, **Bridged Mode Only** (Nur Überbrückungsmodus) oder **IPoA**. Weitere Einzelheiten zu den Einstellungen für die Internetverbindung finden Sie in „Kapitel 6: Konfigurieren des Wireless-G ADSL-Gateways mit SRX200“.
  2. Stellen Sie sicher, dass Sie das richtige Kabel verwenden. Überprüfen Sie, ob die LED **ADSL** des Gateways konstant leuchtet.
  3. Stellen Sie sicher, dass das an den Port **ADSL** des Gateways angeschlossene Kabel in den Splitter des ADSL-Anschlusses eingesteckt ist. Überprüfen Sie, ob auf der Statusseite des webbasierten Dienstprogramms des Gateways eine gültige IP-Adresse des ISP aufgeführt ist.
  4. Schalten Sie den Computer und das Gateway aus. Warten Sie 30 Sekunden, und schalten Sie dann das Gateway und den Computer wieder ein. Überprüfen Sie, ob im webbasierten Dienstprogramm des Gateways auf der Registerkarte **Status** eine IP-Adresse angezeigt wird.

***4. Ich kann nicht auf die Seite „Setup“ (Einrichtung) des webbasierten Dienstprogramms des Gateways zugreifen.***

- Informationen zur Überprüfung einer ordnungsgemäßen Verbindung des Computers mit dem Gateway finden Sie unter „2. Ich möchte meine Internetverbindung prüfen“.
  1. Informationen zur Überprüfung, ob der Computer über eine IP-Adresse, eine Subnetzmaske, ein Gateway und einen DNS verfügt, finden Sie in „Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters“.
  2. Legen Sie eine statische IP-Adresse für de Computer fest. Weitere Informationen hierzu finden Sie unter „1. Wie lege ich eine statische IP-Adresse fest?“.
  3. Befolgen Sie die Anweisungen unter „10. Wie kann ich als PPPoE-Benutzer die Proxy-Einstellungen bzw. das Popup-Fenster für DFÜ-Verbindungen entfernen?“.

***5. Mein VPN (Virtual Private Network) funktioniert nicht über das Gateway.***

Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf, und öffnen Sie die Registerkarte **Security** (Sicherheit). Stellen Sie sicher, dass Sie die Option **IPSec Passthrough** (IPSec-Passthrough) und/oder **PPTP Passthrough** (PPTP-Passthrough) aktiviert haben.

- VPNs, in denen IPSec mit der ESP-Authentifizierung (*Encapsulation Security Payload*, auch als Protokoll 50 bezeichnet) verwendet wird, funktionieren einwandfrei. Über das Gateway wird mindestens eine IPSec-Sitzung übertragen. Je nach den Spezifikationen Ihres VPNs sind jedoch auch zeitgleiche IPSec-Sitzungen möglich.
- VPNs, in denen IPSec und AH (*Authentication Header*, auch als Protokoll 51 bezeichnet) verwendet werden, sind mit dem Gateway nicht kompatibel. Die Verwendung von AH ist aufgrund gelegentlicher Inkompatibilität mit dem NAT-Standard beschränkt.
- Ändern Sie die IP-Adresse des Gateways auf ein anderes Subnetz, sodass Konflikte zwischen der IP-Adresse des VPNs und Ihrer lokalen IP-Adresse vermieden werden. Wenn Ihr VPN-Server beispielsweise die IP-Adresse 192.168.1.X zuweist (wobei „X“ für eine Zahl zwischen 1 und 254 steht) und die IP-Adresse Ihres LANs 192.168.1.X lautet (wobei „X“ mit der in der IP-Adresse des VPNs verwendeten Zahl identisch ist), werden Informationen vom Gateway u. U. nicht richtig übertragen. Zur Problembehebung ändern Sie die IP-Adresse des Gateways in **192.168.2.1**. Ändern Sie die IP-Adresse des Gateways im webbasierten Dienstprogramm auf der Registerkarte **Setup** (Einrichtung).
- Wenn Sie einem Computer oder einem anderen Gerät in Ihrem Netzwerk eine statische IP-Adresse zugewiesen haben, müssen Sie diese IP-Adresse dementsprechend in **192.168.2.Y** (wobei „Y“ für eine Zahl zwischen 1 und 254 steht) ändern. Beachten Sie, dass jede IP-Adresse im Netzwerk eindeutig sein muss.
- Bei Ihrem VPN ist es u. U. erforderlich, dass Pakete für den UDP-Port 500 an den Computer übertragen werden, der mit dem IPSec-Server verbunden ist. Details hierzu finden Sie unter „7. Ich möchte das Hosting für Online-Spiele einrichten bzw. weitere Internetanwendungen verwenden“.
- Weitere Informationen finden Sie auf der Website von Linksys unter www.linksys.com/international.

***6. Wie richte ich einen Server hinter dem Gateway ein und gebe ihn für alle Benutzer frei?***

Um einen Server als Web-, FTP- oder Mail-Server zu verwenden, muss Ihnen die jeweils verwendete Anschlussnummer bekannt sein. Beispiel: Port 80 (HTTP) wird für Webserver, Port 21 (FTP) für FTP-Server und Port 25 (SMTP-Ausgang) sowie Port 110 (POP3-Eingang) für Mail-Server verwendet. Weitere Informationen finden Sie in der Dokumentation des installierten Servers.

- Befolgen Sie die hier aufgeführten Schritte, um die Anschlussweiterleitung über das webbasierte Dienstprogramm des Gateways einzurichten. Im Folgenden finden Sie Anweisungen zum Einrichten von Web-, FTP- und Mailservern.
  1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Rufen Sie unter **Applications and Gaming** (Anwendungen und Spiele) die Registerkarte **Port Range Forwarding** (Weiterleitung an einen Anschlussbereich) auf.
  2. Geben Sie für die benutzerdefinierte Anwendung einen beliebigen Namen ein.
  3. Geben Sie den externen Anschlussbereich für den verwendeten Dienst an. Wenn Sie beispielsweise einen Webserver verwenden, legen Sie den Bereich zwischen 80 und 80 fest.
  4. Aktivieren Sie das zu verwendende Protokoll (TCP und/oder UDP).
  5. Geben Sie die IP-Adresse des Ziel-Computers bzw. -Netzwerkgeräts für den Port-Server ein. Beispiel: Wenn die IP-Adresse für den Ethernet-Adapter des Webservers 192.168.1.100 lautet, geben Sie den Wert **100** in das dafür vorgesehene Feld ein. Weitere Informationen zum Ermitteln von IP-Adressen finden Sie in „Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters“.

6. Aktivieren Sie für die zu verwendenden Anschlussdienste die Option **Enable** (Aktivieren). Beispiel:

| Benutzerdefinierte Anwendung | Externer Anschluss | TCP | UDP | IP-Adresse | Aktivieren |
|---|---|---|---|---|---|
| Webserver | 80 bis 80 | X | | 192.168.1.100 | X |
| FTP-Server | 21 bis 21 | X | | 192.168.1.101 | X |
| SMTP (Ausgang) | 25 bis25 | X | | 192.168.1.102 | X |
| POP3 (Eingang) | 110 bis 110 | X | | 192.168.1.102 | X |

Klicken Sie nach Abschluss der Konfiguration auf die Schaltfläche **Save Settings** (Einstellungen speichern).

***7. Ich möchte das Hosting für Online-Spiele einrichten bzw. weitere Internetanwendungen verwenden.***

Zum Verwenden von Online-Spielen oder Internetanwendungen ist i. d. R. keine Anschlussweiterleitung bzw. kein DMZ-Hosting notwendig. U. u. möchten Sie jedoch gelegentlich selbst Online-Spiele oder Internetanwendungen hosten. Dazu müssen Sie das Gateway so einrichten, dass eingehende Datenpakete oder Daten an einen bestimmten Computer geliefert werden. Dies trifft auch auf die verwendeten Internetanwendungen zu. Sie erhalten Informationen zu den zu verwendenden Anschlussdiensten auf der Website des betreffenden Online-Spiels bzw. der Anwendung, das bzw. die Sie verwenden möchten. Führen Sie diese Schritte aus, um ein Hosting für ein Online-Spiel auszuführen bzw. um eine bestimmte Internetanwendung zu verwenden:

1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Rufen Sie unter **Applications and Gaming** (Anwendungen und Spiele) die Registerkarte **Port Range Forwarding** (Weiterleitung an einen Anschlussbereich) auf.
2. Geben Sie für die benutzerdefinierte Anwendung einen beliebigen Namen ein.
3. Geben Sie den externen Anschlussbereich für den verwendeten Dienst an. Um beispielsweise Unreal Tournament (UT) auszuführen, müssen Sie den Bereich von 7777 bis 27900 eingeben.
4. Aktivieren Sie das zu verwendende Protokoll (TCP und/oder UDP).
5. Geben Sie die IP-Adresse des Ziel-Computers bzw. -Netzwerkgeräts für den Port-Server ein. Beispiel: Wenn die IP-Adresse für den Ethernet-Adapter des Webservers 192.168.1.100 lautet, geben Sie den Wert **100** in das dafür vorgesehene Feld ein. Weitere Informationen zum Ermitteln von IP-Adressen finden Sie in „Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters“.
6. Aktivieren Sie für die zu verwendenden Anschlussdienste die Option **Enable** (Aktivieren). Beispiel:

| Benutzerdefinierte Anwendung | Externer Anschluss | TCP | UDP | IP-Adresse | Aktivieren |
|---|---|---|---|---|---|
| UT | 7777 bis 27900 | X | X | 192.168.1.100 | X |
| Half-Life | 27015 bis 27015 | X | X | 192.168.1.105 | X |
| PCAnywhere | 5631 bis 5631 | | X | 192.168.1.102 | X |
| VPN/IPSEC | 500 bis 500 | | X | 192.168.1.100 | X |

Klicken Sie nach Abschluss der Konfiguration auf die Schaltfläche **Save Settings** (Einstellungen speichern).

***8. Weder Internetspiele, Internetserver noch Internetanwendungen funktionieren.***

Falls Sie Schwierigkeiten haben, Internetspiele, -server und -anwendungen zu verwenden, verbinden Sie einen Computer über das DMZ (*DeMilitarized Zone*)-Hosting mit dem Internet. Diese Option ist verfügbar, wenn für eine Anwendung zu viele Ports erforderlich sind oder Sie nicht sicher sind, welchen Anschlussdienst Sie verwenden sollen. Stellen Sie sicher, dass alle Weiterleitungseinträge deaktiviert sind, um das DMZ-Hosting erfolgreich zu verwenden, da die Weiterleitung Vorrang vor dem DMZ-Hosting hat. (Mit anderen Worten: Für in das Gateway eingehende Daten werden zuerst die Weiterleitungseinstellungen überprüft. Falls die Daten von einer Port-Nummer eingehen, für die keine Anschlussweiterleitung aktiviert ist, sendet das Gateway die Daten an einen beliebigen Computer oder ein beliebiges Netzwerkgerät, der bzw. das für DMZ-Hosting festgelegt wurde.)

- Führen Sie folgende Schritte aus, um DMZ-Hosting festzulegen:
  1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Rufen Sie unter **Applications and Gaming** (Anwendungen und Spiele) die Registerkarte **DMZ** auf. Wählen Sie **Enabled** (Aktiviert) aus, und geben Sie die IP-Adresse des Computers ein.
  2. Überprüfen Sie die Seiten zur Anschlussweiterleitung, und deaktivieren bzw. entfernen Sie die Einträge zur Weiterleitung. Speichern Sie diese Informationen, falls Sie sie zu einem späteren Zeitpunkt verwenden möchten.
- Klicken Sie nach Abschluss der Konfiguration auf die Schaltfläche **Save Settings** (Einstellungen speichern).

***9. Ich habe das Passwort vergessen bzw. die Aufforderung zur Eingabe des Passworts wird jedes Mal angezeigt, wenn ich die Einstellungen für das Gateway speichere.***

- Setzen Sie das Gateway auf die Werkseinstellungen zurück, indem Sie die Reset-Taste 10 Sekunden lang gedrückt halten. Wenn Sie immer noch bei jedem Speichern der Einstellungen zur Eingabe des Passworts aufgefordert werden, führen Sie die folgenden Schritte aus:
  1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Geben Sie den Standardbenutzernamen und das Standardpasswort **admin** ein, und rufen Sie unter **Administration** (Verwaltung) die Registerkarte **Management** (Verwaltungsfunktionen) auf.
  2. Geben Sie im Feld für das Gateway-Passwort ein anderes Passwort ein. Geben Sie anschließend im zweiten Feld das gleiche Passwort ein, um es dadurch zu bestätigen.
  3. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern).

***10. Wie kann ich als PPPoE-Benutzer die Proxy-Einstellungen bzw. das Popup-Fenster für DFÜ-Verbindungen entfernen?***

Wenn Sie Proxy-Einstellungen verwenden, müssen Sie diese auf Ihrem Computer deaktivieren. Da es sich bei dem Gateway um das Gateway für die Internetverbindung handelt, benötigt der Computer keine Proxy-Einstellungen für den Zugriff auf das Internet. Führen Sie die folgenden Anweisungen aus, um sicherzustellen, dass Sie keine Proxy-Einstellungen verwenden und der verwendete Browser direkt eine Verbindung mit dem LAN herstellt.

- Für Benutzer von Microsoft Internet Explorer 5.0 oder höher:
  1. Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf **Internetoptionen**.
  2. Klicken Sie auf die Registerkarte **Verbindungen**.
  3. Klicken Sie auf die Schaltfläche **LAN-Einstellungen**, und deaktivieren Sie alle aktivierten Optionen.
  4. Klicken Sie auf die Schaltfläche **OK**, um zum vorherigen Fenster zu wechseln.
  5. Aktivieren Sie die Option **Keine Verbindung wählen**. Dadurch werden alle Popup-Fenster für DFÜ-Verbindungen für PPPoE-Benutzer entfernt.

- Für Netscape 6 oder höher:
  1. Starten Sie **Netscape Navigator**, und klicken Sie auf **Bearbeiten**, **Einstellungen**, **Erweitert** und **Proxies**.
  2. Stellen Sie sicher, dass in diesem Fenster die Option **Direkte Verbindung zum Internet** ausgewählt ist.
  3. Schließen Sie alle Fenster, um den Vorgang zu beenden.

***11. Ich muss das Gateway auf die Werkseinstellungen zurücksetzen, um den Vorgang noch einmal von vorn zu beginnen.***

Halten Sie die Reset-Taste 10 Sekunden lang gedrückt. Dadurch werden die Interneteinstellungen, das Passwort, die Weiterleitungsfunktion sowie weitere Einstellungen des Gateways auf die Werkseinstellungen zurückgesetzt. Anders ausgedrückt: Das Gateway verwendet wieder die werkseitige Konfiguration.

***12. Ich möchte die Firmware aktualisieren.***

Um die Firmware zu aktualisieren und so die neuesten Funktionen zu erhalten, besuchen Sie die internationale Website von Linksys unter www.linksys.com/international, und laden Sie die neueste Firmware herunter.

- Führen Sie die folgenden Schritte aus:
  1. Wählen Sie auf der internationalen Website von Linksys unter http://www.linksys.com/international Ihre Region bzw. Ihr Land aus.
  2. Klicken Sie auf die Registerkarte **Produkt**, und wählen Sie das Gateway aus.
  3. Klicken Sie auf der Website des Gateways auf **Firmware**, und laden Sie anschließend die aktuelle Firmware für das Gateway herunter.

4. Führen Sie zum Aktualisieren der Firmware die Schritte in „Kapitel 6: Konfigurieren des Wireless-G ADSL-Gateways mit SRX200“ im Abschnitt „Verwaltung“ aus.

***13. Die Aktualisierung der Firmware ist fehlgeschlagen bzw. die Netzstrom-LED blinkt.***

Die Aktualisierung der Firmware kann aus mehreren Gründen fehlschlagen. Führen Sie diese Schritte aus, um die Firmware zu aktualisieren bzw. das Blinken der Netzstrom-LED zu stoppen:

- Wenn die Aktualisierung der Firmware fehlgeschlagen ist, verwenden Sie das TFTP-Programm (das Programm wurde zusammen mit der Firmware heruntergeladen). Öffnen Sie die zusammen mit der Firmware und dem TFTP-Programm heruntergeladene PDF-Datei, und befolgen Sie die darin aufgeführten Anweisungen.
- Legen Sie auf dem Computer eine statische IP-Adresse fest. Folgen Sie dazu den Anweisungen unter „1. Wie lege ich eine statische IP-Adresse auf einem Computer fest?“. Verwenden Sie für den Computer die folgenden Einstellungen für die IP-Adresse:
  IP-Adresse: 192.168.1.50
  Subnetzmaske: 255.255.255.0
  Gateway: 192.168.1.1
- Nehmen Sie die Aktualisierung mithilfe des TFTP-Programms oder auf der Registerkarte **Administration** (Verwaltung) im webbasierten Dienstprogramm des Gateways vor.

***14. Das PPPoE-Protokoll des DSL-Anbieters wird stets unterbrochen.***

PPPoE ist keine dedizierte oder stets aktive Verbindung. Die DSL-Verbindung kann durch den ISP getrennt werden, wenn die Verbindung einige Zeit inaktiv war, ähnlich wie bei einer normalen Telefon-DFÜ-Verbindung zum Internet.

- Es steht eine Setup-Option zur Aufrechterhaltung der Verbindung zur Verfügung. Diese Option funktioniert möglicherweise nicht immer, Sie müssen daher die Verbindung regelmäßig neu herstellen.
  1. Rufen Sie zum Verbinden des Gateways den Web-Browser auf, und geben Sie **http://192.168.1.1** bzw. die IP-Adresse des Gateways ein.
  2. Geben Sie, falls erforderlich, Ihren Benutzernamen und Ihr Passwort ein. (Der Standardbenutzername und das Standardpasswort sind **admin**.)
  3. Wählen Sie im Fenster *Setup* (Einrichtung) die Option **Keep Alive** (Verbindung aufrechterhalten) aus, und legen Sie für die Option **Redial Period** (Wahlwiederholung) 20 Sekunden fest. (Damit wird die Verbindung zum ISP beibehalten, also nicht getrennt.)
  4. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern). Klicken Sie auf die Registerkarte **Status**, und klicken Sie auf Schaltfläche **Connect** (Verbinden).
  5. Möglicherweise wird als Anmeldestatus **Connecting** (Verbindung wird hergestellt) angezeigt. Drücken Sie die Taste F5, um das Fenster zu aktualisieren, bis als Anmeldestatus **Connected** (Verbunden) angezeigt wird.
  6. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um fortzufahren.
- Falls die Verbindung wieder unterbrochen wird, führen Sie die Schritte 1 bis 6 aus, um die Verbindung erneut herzustellen.

***15. Ich kann weder auf meine E-Mail noch auf das Internet oder auf das VPN zugreifen, oder ich empfange nur beschädigte Daten aus dem Internet.***

Sie müssen den Wert für die MTU-Einstellung (*Maximum Transmission Unit*, Maximale Übertragungseinheit) anpassen. Die maximale Übertragungseinheit wird standardmäßig automatisch festgelegt.

- Wenn Sie Schwierigkeiten haben, führen Sie folgende Schritte aus:
  1. Rufen Sie zum Verbinden des Gateways den Web-Browser auf, und geben Sie **http://192.168.1.1** bzw. die IP-Adresse des Gateways ein.
  2. Geben Sie, falls erforderlich, Ihren Benutzernamen und Ihr Passwort ein. (Der Standardbenutzername und das Standardpasswort sind **admin**.)
  3. Wählen Sie für die MTU-Option **Manual** (Manuell) aus. Geben Sie in das Feld **Size** (Größe) den Wert **1492** ein.
  4. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um fortzufahren.
- Wenn das Problem weiterhin besteht, ändern Sie den MTU-Wert auf einen anderen Wert. Verwenden Sie aus der folgenden Liste jeweils einen Wert in der angegebenen Reihenfolge, bis das Problem gelöst ist:
  1462
  1400
  1362
  1300

***16. Die LED Power (Netzstrom) blinkt ständig.***

Die LED **Power** (Netzstrom) leuchtet auf, wenn das Gerät erstmals eingeschaltet wird. Das System wird dann gestartet und auf einen ordnungsgemäßen Betrieb hin geprüft. Nach dem Überprüfungsvorgang leuchtet die LED konstant, wodurch der ordnungsgemäße Betrieb angezeigt wird. Wenn die LED anschließend weiterblinkt, funktioniert das Gerät nicht ordnungsgemäß. Laden Sie die Firmware erneut in den Flash-Speicher, indem Sie dem Computer eine statische IP-Adresse zuweisen und anschließend die Firmware aktualisieren. Verwenden Sie hierfür die folgenden Einstellungen: IP-Adresse **192.168.1.50**, Subnetzmaske **255.255.255.0**.

***17. Bei Eingabe einer URL- oder IP-Adresse erhalte ich eine Meldung, dass eine Zeitüberschreitung vorliegt, bzw. die Aufforderung, den Vorgang erneut auszuführen.***

- Prüfen Sie, ob Sie den Vorgang auf einem anderen Computer ausführen können. Ist dies der Fall, stellen Sie sicher, dass die IP-Einstellungen Ihres Computers korrekt sind (IP-Adresse, Subnetzmaske, Standard-Gateway und DNS). Starten Sie den Computer neu, bei dem das Problem aufgetreten ist.
- Falls der Computer korrekt konfiguriert ist, jedoch immer noch nicht funktioniert, überprüfen Sie das Gateway. Überprüfen Sie, ob es richtig angeschlossen und eingeschaltet ist. Stellen Sie die Verbindung mit dem Router her, und überprüfen Sie die Einstellungen. (Wenn Sie keine Verbindung herstellen können, prüfen Sie die LAN-Verbindung und die Stromversorgung.)
- Wenn das Gateway korrekt konfiguriert ist, prüfen Sie Ihre Internetverbindung (Kabel-/ADSL-Modem usw.), um den ordnungsgemäßen Betrieb des Gateways zu überprüfen. Sie können das Gateway entfernen, um dadurch die direkte Verbindung zu prüfen.

- Konfigurieren Sie die TCP/IP-Einstellung mithilfe einer von Ihrem ISP zur Verfügung gestellten DNS-Adresse manuell.
- Vergewissern Sie sich, dass Ihr Browser die Verbindung direkt herstellt und jegliche DFÜ-Verbindung deaktiviert ist. Wenn Sie Internet Explorer verwenden, klicken Sie auf **Extras**, **Internetoptionen** und anschließend auf die Registerkarte **Verbindungen**. Stellen Sie sicher, dass für Internet Explorer die Option **Keine Verbindung wählen** aktiviert ist. Wenn Sie Netscape Navigator verwenden, klicken Sie auf **Bearbeiten**, **Einstellungen**, **Erweitert** und **Proxies**. Stellen Sie sicher, dass für Netscape Navigator die Option **Direkte Verbindung zum Internet** aktiviert ist.

***18. Beim Versuch, auf das webbasierte Dienstprogramm des Gateways zuzugreifen, wird das Anmeldefenster nicht angezeigt. Stattdessen wird die Meldung „404 Forbidden“ (404 Nicht erlaubt) angezeigt.***

Wenn Sie Internet Explorer verwenden, führen Sie die folgenden Schritte aus, bis das Anmeldefenster des webbasierten Dienstprogramms angezeigt wird (bei Verwendung von Netscape Navigator sind ähnliche Schritte erforderlich):

1. Klicken Sie auf **Datei**. Stellen Sie sicher, dass *Offlinebetrieb* NICHT aktiviert ist.
2. Drücken Sie **Strg + F5**. Dadurch wird eine Aktualisierung erzwungen und Internet Explorer veranlasst, neue und nicht gespeicherte Websites zu laden.

- Klicken Sie auf **Extras**. Klicken Sie auf **Internetoptionen**. Klicken Sie auf die Registerkarte **Sicherheit**. Klicken Sie auf die Schaltfläche **Standardstufe**. Stellen Sie sicher, dass die Sicherheitsstufe auf **Mittel** oder niedriger festgelegt ist. Klicken Sie anschließend auf die Schaltfläche **OK**.

## Häufig gestellte Fragen

***Wie viele IP-Adressen kann das Gateway maximal unterstützen?***
Das Gateway unterstützt bis zu 253 IP-Adressen.

***Unterstützt das Gateway IPSec-Passthrough?***
Ja, dabei handelt es sich um eine integrierte Funktion, die standardmäßig aktiviert ist.

***An welcher Stelle im Netzwerk wird das Gateway installiert?***
In einer typischen Umgebung wird das Gateway zwischen dem ADSL-Splitter und dem LAN installiert.

***Unterstützt das Gateway IPX oder AppleTalk?***
Nr. TCP/IP ist der einzige Internetprotokollstandard und ist heutzutage globaler Kommunikationsstandard. IPX ist ein Kommunikationsprotokoll von NetWare, das nur zur Weiterleitung von Nachrichten von einem Knotenpunkt zum nächsten verwendet wird. AppleTalk ist ein Kommunikationsprotokoll, das in Apple- und Macintosh-Netzwerken für LAN-zu-LAN-Verbindungen verwendet wird. Beide Protokolle können jedoch nicht zur Verbindung des Internets an ein LAN verwendet werden.

***Unterstützt die LAN-Verbindung des Gateways 100-Mbit/s-Ethernet?***
Das Gateway unterstützt über den EtherFast 10/100-Switch mit Auto-Sensing-Funktion auf der LAN-Seite des Gateways auch 100 Mbit/s.

***Was ist die Netzwerk-Adressen-Übersetzung, und wofür wird sie verwendet?***
Die NAT-Funktion (*Network Address Translation*, Netzwerk-Adressen-Übersetzung) übersetzt mehrere IP-Adressen in einem privaten LAN in eine öffentliche Adresse, die im Internet verwendet wird. Dadurch wird die Sicherheit erhöht, da die Adresse eines mit dem privaten LAN verbundenen Computers nie an das Internet übertragen wird. Darüber hinaus ermöglicht der Einsatz von NAT die Verwendung kostengünstiger Internetverbindungen, wenn nur eine TCP/IP-Adresse vom ISP zur Verfügung gestellt wurde. So können Benutzer mehrere private IP-Adressen hinter einer einzigen vom ISP zur Verfügung gestellten IP-Adresse verwenden.

***Unterstützt das Gateway auch andere Betriebssysteme als Windows 98 SE, ME, 2000 oder XP?***
Ja. Linksys bietet jedoch derzeit keinen technischen Support hinsichtlich Installation, Konfiguration oder Fehlersuche für andere Betriebssysteme als die Windows-Betriebssysteme an.

***Unterstützt das Gateway die ICQ-Dateiübertragung?***
Ja, führen Sie dazu folgende Schritte aus: Klicken Sie auf das Menü **ICQ**, **Preferences** (Einstellungen) und auf **Connection Settings** (Verbindungseinstellungen). Aktivieren Sie dann die Option **Using Firewall/Using Proxy** (Verwendung einer Firewall oder eines Proxy). Legen Sie nun in den Firewall-Einstellungen für die Zeitüberschreitung 80 Sekunden fest. Der Internetbenutzer kann nun Dateien an Benutzer hinter dem Gateway senden.

***Ich habe einen Unreal Tournament-Server eingerichtet, andere Benutzer im LAN können jedoch keine Verbindung mit dem Server herstellen. Was muss ich tun?***
Nach der Installation eines dedizierten Unreal Tournament-Servers müssen Sie eine statische IP-Adresse für jeden Computer im LAN erstellen sowie die Ports 7777, 7778, 7779, 7780, 7781 und 27900 an die IP-Adresse des Servers weiterleiten. Sie können hierfür auch einen Bereich zwischen 7777 und 27900 festlegen. Um die Funktion für UT Server Admin zu verwenden, müssen Sie die Weiterleitung an einen weiteren Port vornehmen. (Das kann Port 8080 sein, der jedoch auch für die Remote-Verwaltung verwendet wird. Sie müssen u. U. diesen Port deaktivieren.) Legen Sie anschließend in der Datei SERVER.INI im Abschnitt [UWeb.WebServer] für „ListenPort“ den Wert 8080 (in Übereinstimmung mit dem oben erwähnten zugeordneten Port) und für „ServerName“ die von Ihrem ISP zur Verfügung gestellte IP-Adresse des Gateways fest.

***Können mehrere Spieler im LAN auf einen Spieleserver zugreifen und mit nur einer öffentlichen IP-Adresse gleichzeitig spielen?***
Das hängt vom verwendeten Netzwerkspiel bzw. dem verwendeten Server ab. So unterstützt z. B. Unreal Tournament das mehrfache Anmelden mit nur einer öffentlichen IP-Adresse.

***Wie kann ich Half-Life – Team Fortress mit dem Gateway verwenden?***
Der standardmäßige Client-Port für Half-Life ist 27005. Für die Computer in Ihrem LAN muss in der Befehlszeile für Half-Life-Verknüpfungen „+clientport 2700x“ hinzugefügt werden, wobei „x“ dann 6, 7, 8 usw. entspricht. Dadurch können mehrere Computer mit dem gleichen Server eine Verbindung herstellen. Problem: Bei Version 1.0.1.6 können mehrere Computer, die die gleiche CD-Kennnummer verwenden, nicht gleichzeitig mit dem Server verbunden sein, auch wenn sie sich im gleichen LAN befinden. Dieses Problem tritt bei Version 1.0.1.3 nicht auf. Beim Hosting von Spielen muss sich der Half-Life-Server jedoch nicht in der DMZ befinden. Es muss lediglich der Port 27015 an die lokale IP-Adresse des Server-Computers weitergeleitet werden.

***Die Webseite reagiert nicht, heruntergeladene Dateien sind beschädigt, oder es werden nur unleserliche Zeichen auf dem Bildschirm angezeigt. Was muss ich tun?***
Legen Sie für den Ethernet-Adapter 10 MBit/s bzw. den Halbduplex-Modus fest, und deaktivieren Sie als vorübergehende Maßnahme für den Ethernet-Adapter die Funktion zur automatischen Verbindungsaushandlung. (Rufen Sie in der Systemsteuerungskomponente **Netzwerk** die Registerkarte für die erweiterten Einstellungen des Ethernet-Adapters auf.) Stellen Sie sicher, dass die Proxy-Einstellung im Browser deaktiviert ist. Weitere Informationen erhalten Sie unter www.linksys.com/international.

***Was kann ich tun, wenn alle Maßnahmen bei einer fehlgeschlagenen Installation erfolglos bleiben?***
Setzen Sie das Gateway auf die Werkseinstellungen zurück, indem Sie die Taste **Reset** drücken, bis die LED **Power** (Netzstrom) aufleuchtet und wieder erlischt. Setzen Sie das ADSL-Modem zurück, indem Sie es aus- und erneut einschalten. Laden Sie die neueste Firmware-Version über die internationale Website von Linksys unter www.linksys.com/international herunter, und nehmen Sie die Aktualisierung vor.

***Wie erhalte ich Informationen zu neuen Aktualisierungen der Gateway-Firmware?***
Sämtliche Aktualisierungen für Firmware von Linksys werden auf der internationalen Website von Linksys unter www.linksys.com/international veröffentlicht und können kostenlos heruntergeladen werden. Verwenden Sie zur Aktualisierung der Gateway-Firmware die Registerkarte **System** des webbasierten Dienstprogramms des Gateways. Wenn die Internetverbindung des Gateways zufriedenstellend funktioniert, besteht keine Notwendigkeit, eine neuere Firmware-Version herunterzuladen, es sei denn, Sie möchten neue Funktionen der aktualisierten Version verwenden.

***Funktioniert das Gateway in einer Macintosh-Umgebung?***
Ja, Sie können jedoch nur über Internet Explorer 4.0 bzw. Netscape Navigator 4.0 oder höher für Macintosh auf die Setup-Seiten des Gateways zugreifen.

***Ich kann die Seite für die Webkonfiguration des Gateways nicht aufrufen. Was kann ich tun?***
Sie müssen möglicherweise die Proxy-Einstellungen in Ihrem Internet-Browser, z. B. Netscape Navigator oder Internet Explorer, entfernen. Weitere Anweisungen erhalten Sie in der Dokumentation zu Ihrem Browser. Stellen Sie sicher, dass Ihr Browser die Verbindung direkt herstellt und jegliche DFÜ-Verbindung deaktiviert ist. Wenn Sie Internet Explorer verwenden, klicken Sie auf **Extras**, **Internetoptionen** und anschließend auf die Registerkarte **Verbindungen**. Stellen Sie sicher, dass für Internet Explorer die Option **Keine Verbindung wählen** aktiviert ist. Wenn Sie Netscape Navigator verwenden, klicken Sie auf **Bearbeiten**, **Einstellungen**, **Erweitert** und **Proxies**. Stellen Sie sicher, dass für Netscape Navigator die Option **Direkte Verbindung zum Internet** aktiviert ist.

***Was bedeutet DMZ-Hosting?***
Mithilfe der DMZ (*Demilitarized Zone*, Entmilitarisierte Zone) kann über eine IP-Adresse (d. h. über einen Computer) eine Verbindung zum Internet hergestellt werden. Für einige Anwendungen ist es erforderlich, dass mehrere TCP/IP-Ports geöffnet sind. Es ist empfehlenswert, dass Sie zur Verwendung des DMZ-Hostings für Ihren Computer eine statische IP-Adresse festlegen. Weitere Informationen zum Ermitteln einer LAN-IP-Adresse finden Sie in „Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters“.

***Verwenden bei DMZ-Hosting sowohl DMZ-Benutzer als auch Gateway die öffentliche IP-Adresse?***
Nr.

***Leitet das Gateway PPTP-Datenpakete oder PPTP-Sitzungen aktiv weiter?***
Durch das Gateway werden PPTP-Datenpakete weitergeleitet.

***Ist das Gateway auch plattformübergreifend einsetzbar?***
Jede Plattform, die Ethernet und TCP/IP unterstützt, ist mit dem Gateway kompatibel.

***Wie viele Ports können gleichzeitig weitergeleitet werden?***
Das Gateway kann theoretisch 520 Sitzungen gleichzeitig ausführen, Sie können jedoch nur 10 Anschlussbereiche weiterleiten.

***Über welche erweiterten Funktionen verfügt das Gateway?***
Zu den erweiterten Funktionen des Gateways zählen u. a. erweiterte Wireless-Einstellungen, Filter, Port-Forwarding, Routing und DDNS.

**Wie kann ich überprüfen, ob ich über statische oder DHCP-IP-Adressen verfüge?**
Wenden Sie sich an Ihren ISP, um diese Informationen zu erhalten.

***Wie kann ich mIRC mit dem Gateway verwenden?***
Legen Sie auf der Registerkarte **Port Forwarding** (Anschlussweiterleitung) den Wert **113** für den Computer fest, auf dem Sie mIRC verwenden möchten.

***Kann das Gateway als DHCP-Server eingesetzt werden?***
Ja. Das Gateway verfügt über eine integrierte DHCP-Server-Software.

***Kann ich Anwendungen von Remote-Computern über das Wireless-Netzwerk ausführen?***
Dies ist abhängig davon, ob die Anwendung für die Verwendung in Netzwerken entwickelt wurde. Informationen dazu, ob die Anwendung in Netzwerken verwendet werden kann, finden Sie in der Dokumentation der entsprechenden Anwendung.

***Was ist der IEEE 802.11g-Standard?***
Dies ist ein IEEE-Standard für Wireless-Netzwerke. Mit dem 802.11g-Standard können Geräte von unterschiedlichen Herstellern im Wireless-Netzwerk miteinander kommunizieren, sofern die Geräte mit dem 802.11g-Standard kompatibel sind. Durch den 802.11g-Standard ist eine maximale Datenübertragungsrate von 54 MBit/s und eine Betriebsfrequenz von 2,4 GHz vorgegeben.

***Was ist der IEEE 802.11b-Standard?***
Dies ist ein IEEE-Standard für Wireless-Netzwerke. Mit dem 802.11b-Standard können Geräte von unterschiedlichen Herstellern im Wireless-Netzwerk miteinander kommunizieren, sofern die Geräte mit dem 802.11b-Standard kompatibel sind. Durch den 802.11b-Standard ist eine maximale Datenübertragungsrate von 11 MBit/s und eine Betriebsfrequenz von 2,4 GHz vorgegeben.

***Welche IEEE 802.11b- und 802.11g-Funktionen werden unterstützt?***
Das Produkt unterstützt die folgenden IEEE 802.11b- und IEEE 802.11g-Funktionen:

- CSMA/CA sowie das Acknowledge-Protokoll
- Multi-Channel-Roaming
- Automatische Ratenauswahl
- RTS/CTS
- Fragmentierung
- Energieverwaltung

Es unterstützt zudem die OFDM-Technologie für 802.11g-Netzwerke.

***Was bedeutet Ad-hoc-Modus?***
Wenn für ein Wireless-Netzwerk der Ad-hoc-Modus festgelegt ist, sind die Wireless-Computer so konfiguriert, dass sie ohne Access Point direkt miteinander kommunizieren (Peer-to-Peer).

***Was bedeutet Infrastrukturmodus?***
Wenn für ein Wireless-Netzwerk der Infrastrukturmodus festgelegt wurde, ist es so konfiguriert, dass es über einen Wireless Access Point mit Netzwerken kommuniziert.

***Was ist Roaming?***

Roaming ermöglicht Benutzern von tragbaren Computern einen reibungslosen Datenaustausch beim Zurücklegen von Entfernungen, die nicht von einem einzigen Access Point abgedeckt werden können. Vor Verwendung des Roamings muss der Computer auf die gleiche Kanalnummer wie der Access Point des entsprechenden Empfangsbereichs gesetzt werden.

Um eine dauerhafte nahtlose Verbindung zu erzielen, muss das Wireless-LAN eine Reihe an unterschiedlichen Funktionen besitzen. So müssen z. B. alle Nachrichten von jedem Knoten und jedem Access Point bestätigt werden. Jeder Knoten muss den Kontakt mit dem Wireless-Netzwerk aufrechterhalten, auch wenn keine Datenübertragung stattfindet. Damit diese Funktionen gleichzeitig ausgeführt werden können, ist eine dynamische Funkfrequenz-Netzwerktechnologie erforderlich, mit der Access Points und Knoten miteinander verknüpft werden. In solchen Systemen sucht der Endknoten des Benutzers nach dem jeweils besten Zugriff auf das System. Zunächst werden Faktoren wie Signalstärke und -qualität, die aktuelle Nachrichtenmenge, die von jedem Access Point verarbeitet wird, und die Entfernung zwischen jedem Access Point zum verdrahteten Backbone ausgewertet. Anschließend ermittelt der Knoten auf Grundlage dieser Informationen den geeigneten Access Point und registriert dessen Adresse. Die Kommunikation zwischen Knoten und Host-Computer kann in beide Richtungen des Backbones verlaufen.

Bei fortschreitender Kommunikation prüft der Funkfrequenz-Sender des Endknotens in regelmäßigen Abständen, ob eine Verbindung mit dem ursprünglichen Access Point vorliegt oder ob ein neuer Access Point gesucht werden soll. Wenn ein Knoten keine Bestätigung des ursprünglichen Access Point mehr erhält, wird eine neue Verbindungssuche gestartet. Sobald ein neuer Access Point gefunden wurde, wird dessen Adresse registriert und die Kommunikation fortgesetzt.

***Was bedeutet ISM-Band?***

Die FCC-Behörde und die jeweiligen Behörden außerhalb der USA haben Bestimmungen hinsichtlich der Bandbreite für eine nicht durch Lizenzen abgedeckte Verwendung im ISM-Band erlassen. Die Frequenz liegt bei ca. 2,4 GHz und kann weltweit genutzt werden. Mit dieser wahrlich revolutionären Maßnahme können nun problemlos High Speed-Wireless-Funktionen von Benutzern weltweit genutzt werden.

***Was bedeutet Bandspreizung?***

Die Technologie der Bandspreizung (*Spread Spectrum Technology*) ist eine vom Militär entwickelte Breitband-Funkfrequenz-Technologie, die für zuverlässige, sichere und störresistente Kommunikationssysteme eingesetzt werden kann. Bei dieser Technologie werden gewisse Abstriche bei der Bandbreiteneffizienz hingenommen, um eine höhere Zuverlässigkeit, Integrität und Sicherheit zu erreichen. Es wird hier also eine größere Bandbreite als bei der Schmalbandübertragung verwendet. Im Gegenzug wird jedoch ein Signal erreicht, das lauter und einfacher zu lokalisieren ist, allerdings unter der Voraussetzung, dass der Empfänger die Parameter des mittels Bandspreizung übertragenen Signals kennt. Wenn ein Empfänger nicht auf die richtige Frequenz eingestellt ist, scheint ein mittels Bandspreizung übertragenes Signal nichts anderes als ein Hintergrundgeräusch zu sein. Es stehen zwei unterschiedliche Verfahren für die Bandspreizung zur Verfügung: DSSS (*Direct Sequence Spread Spectrum*, Direkte Bandspreizung) und FHSS (*Frequency Hopping Spread Spectrum*, Frequenzsprungverfahren).

***Was ist DSSS? Was ist FHSS? Worin liegt der Unterschied?***

Bei FHSS wird ein Schmalbandträger verwendet, der nach einem für Sender und Empfänger bekannten Muster die Frequenz ändert. Bei ordnungsgemäßer Synchronisation wird jeweils ein einziger logischer Kanal aufrechterhalten. Unerwünschten Empfängern erscheint das FHSS-Signal als kurzzeitiges Impulsrauschen. DSSS generiert ein redundantes Bitmuster für jedes zu übertragende Bit. Dieses Bitmuster wird „Chip“ oder „Chipping Code“ genannt. Je länger der Chip ist, desto größer ist die Wahrscheinlichkeit, dass die ursprüngliche Information wieder generiert werden kann. Auch wenn ein oder mehrere Bits im Chip während der Übertragung beschädigt wurden, können diese durch eine statistische Technik im Empfänger regeneriert werden und müssen daher nicht nochmals übertragen werden. Unerwünschten Empfängern erscheint das DSSS-Signal als schwaches Breitbandrauschen und wird von den meisten Schmalbandempfängern ignoriert.

***Können die Daten bei der Funkübertragung abgefangen werden?***

WLAN verfügt über zweifachen Schutz im Sicherheitsbereich. Im Hardwarebereich sorgt DSSS-Technologie (*Direct Sequence Spread Spectrum*, Direkte Bandspreizung) für die integrierte Sicherheitsfunktion der Verschlüsselung. Im Softwarebereich bietet WLAN die WEP-Verschlüsselungsfunktion, um die Sicherheit zu erhöhen und die Zugriffssteuerung zu verbessern.

***Was ist WEP?***

WEP ist die Abkürzung für *Wired Equivalent Privacy*. Hierbei handelt es sich um einen Datenschutzmechanismus, der auf einem 64-Bit- oder 128-Bit-Algorithmus mit gemeinsam verwendetem Schlüssel basiert und im IEEE 802.11-Standard festgelegt ist.

***Was ist eine MAC-Adresse?***

Eine MAC-Adresse (*Media Access Control*) ist eine eindeutige Nummer, die jedem Ethernet-Netzwerkgerät, wie z. B. einem Netzwerkadapter, vom Hersteller zugewiesen wird und mit der das Gerät im Netzwerk auf Hardware-Ebene identifiziert werden kann. Aus praktischen Gründen wird diese Nummer dauerhaft vergeben. Im Gegensatz zu IP-Adressen, die sich bei jeder Anmeldung des Computers beim Netzwerk ändern können, bleibt die MAC-Adresse eines Geräts stets gleich und ist dadurch eine äußerst nützliche Kennung im Netzwerk.

***Wie setze ich das Gateway zurück?***

Halten Sie die Taste **Reset** an der Rückseite des Gateways ca. 10 Sekunden lang gedrückt. Dadurch wird das Gateway auf die Werkseinstellungen zurückgesetzt.

***Wie behebe ich Probleme wegen zu schwachen Signals?***
Sie können die genaue Reichweite Ihres Wireless-Netzwerks nur durch Testen bestimmen. Jedes Hindernis zwischen dem Gateway und einem Wireless-Computer führt zu Signalverlust. Durch verbleites Glas, Metall, Betonböden, Wasser und Wände werden Signale behindert und die Reichweite vermindert. Verwenden Sie das Gateway und den Wireless-Computer zunächst im gleichen Zimmer, und vergrößern Sie dann schrittweise den Abstand zwischen beiden Geräten, um so die maximale Reichweite in Ihrer Umgebung zu bestimmen.

Verwenden Sie auch unterschiedliche Kanäle, da so Störungen ausgeschlossen werden, die nur einen Kanal betreffen.

***Die Signalstärke ist absolut ausreichend, das Netzwerk wird jedoch nicht angezeigt.***
Sicherheit im Wireless-Netzwerkbetrieb ist vermutlich im Gateway, jedoch nicht im Wireless-Adapter (oder umgekehrt) aktiviert. Stellen Sie sicher, dass für alle Geräte in Ihrem Wireless-Netzwerk dieselben Wireless-Sicherheitseinstellungen verwendet werden.

***Wie viele Kanäle/Frequenzen stehen für das Gateway zur Verfügung?***
In weiten Teilen Nord-, Mittel- und Südamerikas sind insgesamt 11 Kanäle (von 1 bis 11) verfügbar. Im Großteil von Europa stehen 13 Kanäle (von 1 bis 13) zur Verfügung. Je nach den regionalen bzw. nationalen Bestimmungen können in anderen Regionen weitere Kanäle verfügbar sein.

Falls Sie hier keine Antworten auf Ihre Fragen erhalten haben, finden Sie weitere Informationen auf der internationalen Website von Linksys unter http://www.linksys.com/international.

# Anhang B: Wireless-Sicherheit

Linksys hat es sich zum Ziel gesetzt, den Wireless-Netzwerkbetrieb für Sie so sicher und einfach wie möglich zu gestalten. Die aktuellen Produkte von Linksys bieten verschiedene Netzwerksicherheitsfunktionen. Um diese anzuwenden, müssen Sie jedoch bestimmte Schritte ausführen. Beachten Sie daher Folgendes beim Einrichten bzw. Verwenden Ihres Wireless-Netzwerks.

## Vorsichtsmaßnahmen

Bei der folgenden Liste handelt es sich um eine Auflistung aller möglichen Vorsichtsmaßnahmen. Die Schritte 1 bis 5 sollten Sie unbedingt ausführen:

1. Ändern Sie die Standard-SSID.
2. Deaktivieren Sie die SSID-Übertragung.
3. Ändern Sie das Standardpasswort für das Administratorkonto.
4. Aktivieren Sie die MAC-Adressfilterung.
5. Ändern Sie die SSID regelmäßig.
6. Verwenden Sie den stärksten verfügbaren Verschlüsselungsalgorithmus. Verwenden Sie WPA (falls verfügbar). Beachten Sie, dass die Netzwerkleistung hierdurch verringert werden kann.
7. Ändern Sie die WEP-Verschlüsselungsschlüssel regelmäßig.

Informationen zum Umsetzen dieser Sicherheitsmaßnahmen finden Sie in „Kapitel 6: Konfigurieren des Wireless-G ADSL-Gateways mit SRX200“.

**HINWEIS:** Einige dieser Sicherheitsfunktionen sind nur über das Netzwerk-Gateway, den Router oder den Access Point verfügbar. Weitere Informationen finden Sie in der Dokumentation zum Gateway, Router bzw. Access Point.

## Sicherheitsrisiken bei Wireless-Netzwerken

Wireless-Netzwerke sind einfach zu finden. Hacker wissen, dass Geräte für den Wireless-Netzwerkbetrieb nach so genannten Beacon-Meldungen suchen, bevor sie sich in ein Wireless-Netzwerk einklinken. Diese Meldungen, die umfassende Netzwerkinformationen wie beispielsweise die SSID (*Service Set IDentifier*) des Netzwerks enthalten, lassen sich leicht entschlüsseln. Dagegen können Sie sich folgendermaßen schützen:

**Ändern Sie das Administratorpasswort regelmäßig:** Bedenken Sie, dass bei jedem im Wireless-Netzwerkbetrieb verwendeten Gerät die Netzwerkeinstellungen (SSID, WEP-Schlüssel usw.) in der Firmware gespeichert sind. Die Netzwerkeinstellungen können nur vom Netzwerkadministrator geändert werden. Wenn einem Hacker das Administratorpasswort bekannt wird, kann auch er diese Einstellungen ändern. Deshalb sollten Sie es ihm so schwer wie möglich machen, an diese Informationen zu gelangen. Ändern Sie das Administratorpasswort regelmäßig:

**SSID:** Im Zusammenhang mit der SSID ist Folgendes zu beachten:

1. Deaktivieren Sie die Übertragung.
2. Wählen Sie eine individuelle SSID.
3. Ändern Sie sie regelmäßig.

Bei den meisten Geräten für den Wireless-Netzwerkbetrieb gibt es die Option, die SSID zu übertragen. Diese Option ist zwar recht praktisch, bedeutet jedoch, dass sich jeder in Ihr Wireless-Netzwerk einklinken kann. Jeder, auch Hacker. Daher sollten Sie die SSID nicht übertragen.

Geräte für den Wireless-Netzwerkbetrieb sind werkseitig auf eine Standard-SSID eingestellt. (Die Standard-SSID von Linksys lautet „linksys“.) Hacker kennen diese Standardeinstellungen und können Ihr Netzwerk darauf überprüfen. Ändern Sie Ihre SSID in einen eindeutigen Namen, der keinerlei Bezug zu Ihrem Unternehmen oder zu den von Ihnen verwendeten Netzwerkprodukten hat.

Ändern Sie Ihre SSID regelmäßig, damit Hacker, die sich Zugriff auf Ihr Wireless-Netzwerk verschafft haben, erneut das Passwort knacken müssen.

**MAC-Adressen:** Aktivieren Sie die MAC-Adressfilterung. Durch die MAC-Adressfilterung wird nur Wireless-Knoten mit bestimmten MAC-Adressen der Zugriff auf das Netzwerk ermöglicht. Dies erschwert es Hackern, mit einer zufällig gewählten MAC-Adresse auf Ihr Netzwerk zuzugreifen.

**WEP Encryption (WEP-Verschlüsselung):** WEP (*Wired Equivalent Privacy*) wird oft als eine Art Allheilmittel im Zusammenhang mit Sicherheitsrisiken bei Wireless-Geräten angesehen. Damit werden die Fähigkeiten von WEP jedoch überschätzt. Auch WEP kann nur soweit zur Sicherheit beitragen, dass es Hackern das Eindringen erschwert.

Es gibt mehrere Methoden, um die Wirksamkeit von WEP zu optimieren:

1. Verwenden Sie die höchste Verschlüsselungsebene.
2. Verwenden Sie die Authentifizierung mit einem gemeinsamen Schlüssel.
3. Ändern Sie Ihren WEP-Schlüssel regelmäßig.

**WICHTIG:** Jedes Gerät im Wireless-Netzwerk MUSS dasselbe Verschlüsselungsverfahren und denselben Verschlüsselungsschlüssel verwenden, damit das Wireless-Netzwerk ordnungsgemäß funktioniert.

**WPA:** Bei WPA (Wi-Fi Protected Access) handelt es sich um den neuesten und besten verfügbaren Standard für Wi-Fi-Sicherheit. **WPA2** ist eine neuere Version von WPA (Wi-Fi Protected Access) mit stärkerer Verschlüsselung. Im Modus WPA stehen Ihnen zwei Verschlüsselungsverfahren zur Verfügung: TKIP (Temporal Key Integrity Protocol) und AES (Advanced Encryption System). TKIP verwendet eine leistungsfähigere Verschlüsselungsmethode sowie MIC (Message Integrity Code), um das System gegen Hacker zu schützen. AES arbeitet mit einer symmetrischen blockweisen Datenverschlüsselung mit 128-Bit-Schlüsseln. WPA Enterprise und WPA2 Enterprise verwenden RADIUS (Remote Authentication Dial-In User Service) für die Authentifizierung.

**WPA Personal**: Wählen Sie den gewünschten Algorithmus (**TKIP** oder **AES**) aus, geben Sie im Feld **Passphrase** ein Passwort mit einer Länge von 8 bis 63 Zeichen ein, und legen Sie für **Group Key Renewal** (Erneuerung Gruppenschlüssel) einen Zeitraum zwischen 0 und 99.999 Sekunden fest. Diese Zeitangabe teilt dem Gateway bzw. einem anderen Gerät mit, wie oft die Verschlüsselungsschlüssel gewechselt werden sollen.

**WPA2 Personal**: Bei WPA2 steht Ihnen die Verschlüsselungsmethode TKIP mit dynamischen Verschlüsselungsschlüsseln zur Verfügung. Geben Sie ein Passphrase von 8 bis 63 Zeichen ein. Legen Sie anschließend den Zeitraum für **Group Key Renewal** (Erneuerung Gruppenschlüssel) fest. Diese Zeitangabe teilt dem Gateway mit, wie oft die Verschlüsselungsschlüssel auszutauschen sind.

**WPA2 Mixed Mode** (WPA2 Gemischter Modus): Im gemischten WPA2-Modus stehen TKIP- und AES-Verschlüsselung zur Verfügung. Geben Sie ein Passphrase von 8 bis 63 Zeichen ein. Legen Sie anschließend den Zeitraum für **Group Key Renewal** (Erneuerung Gruppenschlüssel) fest. Diese Zeitangabe teilt dem Gateway mit, wie oft die Verschlüsselungsschlüssel auszutauschen sind.

**WPA Enterprise**: Bei dieser Methode wird WPA in Kombination mit einem RADIUS-Server eingesetzt. Geben Sie die IP-Adresse und die Port-Nummer des RADIUS-Servers ein und dann den Schlüssel, der vom Gateway und dem zugehörigen RADIUS-Server gemeinsam verwendet wird. Legen Sie anschließend den Zeitraum für **Key Renewal Timeout** (Wartezeit für Schlüsselerneuerung) fest. Diese Zeitangabe teilt dem Gateway mit, wie oft die Verschlüsselungsschlüssel auszutauschen sind.

**WPA2 Enterprise**: Bei dieser Methode wird WPA2 in Kombination mit einem RADIUS-Server eingesetzt. Geben Sie die IP-Adresse und die Port-Nummer des RADIUS-Servers ein und dann den Schlüssel, der vom Gateway und dem zugehörigen RADIUS-Server gemeinsam verwendet wird. Legen Sie anschließend den Zeitraum für **Key Renewal Timeout** (Wartezeit für Schlüsselerneuerung) fest. Diese Zeitangabe teilt dem Gateway mit, wie oft die Verschlüsselungsschlüssel auszutauschen sind.

Die Verwendung von Verschlüsselungsfunktionen kann sich negativ auf die Netzwerkleistung auswirken. Wenn Sie jedoch sensible Daten über das Netzwerk senden, sollten Sie diese verschlüsseln.

Wenn Sie diese Sicherheitsempfehlungen einhalten, können Sie ganz beruhigt arbeiten und die flexible und praktische Technologie von Linksys bedenkenlos einsetzen.

# Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters

In diesem Abschnitt wird beschrieben, wie Sie die MAC-Adresse für den Ethernet-Adapter Ihres Computers ermitteln, um die MAC-Filterungsfunktion des Gateways verwenden zu können. Sie können außerdem die IP-Adresse für den Ethernet-Adapter Ihres Computers ermitteln. Die IP-Adresse wird für die Filterungs-, Weiterleitungs- und DMZ-Funktionen des Gateways verwendet. Führen Sie die in diesem Anhang aufgelisteten Schritte aus, um die MAC- oder IP-Adresse des Adapters unter Windows 98, ME, 2000 bzw. XP zu ermitteln.

## Anweisungen für Windows 98/ME

1. Klicken Sie auf **Start** und **Ausführen**. Geben Sie im Feld *Öffnen* den Eintrag **winipcfg** ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**.

2. Wählen Sie im Fenster *IP-Konfiguration* den Ethernet-Adapter aus, den Sie über ein Ethernet-Netzwerkkabel der Kategorie 5 mit dem Gateway verbunden haben. Siehe Abbildung C-1.

3. Notieren Sie die Adapteradresse so, wie sie am Computer angezeigt wird (siehe Abbildung C-2). Dies ist die MAC-Adresse Ihres Ethernet-Adapters und wird im hexadezimalen Format als Folge von Ziffern und Buchstaben dargestellt.

   Die MAC-Adresse/Adapteradresse ist der Wert, der für die MAC-Filterung verwendet wird. Bei dem Beispiel in Abbildung C-2 lautet die MAC-Adresse des Ethernet-Adapters 00-00-00-00-00-00. Die auf Ihrem Computer angezeigte Adresse wird anders lauten.

   Bei dem Beispiel in Abbildung C-2 lautet die IP-Adresse des Ethernet-Adapters 192.168.1.100. Die auf Ihrem Computer angezeigte Adresse kann davon abweichen.

**HINWEIS:** Die MAC-Adresse wird auch als Adapteradresse bezeichnet.

**Abbildung C-1: IP-Konfiguration**

**Abbildung C-2: MAC-Adresse/ Adapteradresse**

## Anweisungen für Windows 2000/XP

1. Klicken Sie auf **Start** und **Ausführen**. Geben Sie im Feld *Öffnen* den Eintrag **cmd** ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**.

**HINWEIS:** Die MAC-Adresse wird auch als physische Adresse bezeichnet.

2. Geben Sie in die Eingabeaufforderung **ipconfig /all** ein. Drücken Sie die Eingabetaste.

3. Notieren Sie die physische Adresse so, wie sie am Computer anzeigt wird (Abbildung C-3). Diese Adresse stellt die MAC-Adresse des Ethernet-Adapters dar. Sie wird als Folge von Ziffern und Buchstaben dargestellt.

   Die MAC-Adresse/physische Adresse ist der Wert, der für die MAC-Filterung verwendet wird. Bei dem Beispiel in Abbildung C-3 lautet die MAC-Adresse des Ethernet-Adapters 00-00-00-00-00-00. Die auf Ihrem Computer angezeigte Adresse wird anders lauten.

   Bei dem Beispiel in Abbildung C-3 lautet die IP-Adresse des Ethernet-Adapters 192.168.1.100. Die auf Ihrem Computer angezeigte Adresse kann davon abweichen.

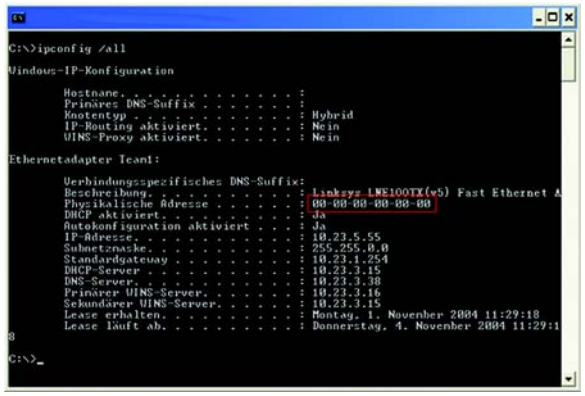
C:\>ipconfig /all
Windows-IP-Konfiguration
Hostname . . . . . :
Primäres DNS-Suffix . . . . . :
Knotentyp . . . . . : Hybrid
IP-Routing aktiviert. . . . . : Nein
WINS-Proxy aktiviert. . . . . : Nein
Ethernetadapter Team1:
Verbindungsspezifisches DNS-Suffix:
Beschreibung . . . . . : Linksys LNE100TX(v5) Fast Ethernet A
Physikalische Adresse . . . . . : 00-00-00-00-00-00
DHCP aktiviert. . . . . : Ja
Autokonfiguration aktiviert . . . : Ja
IP-Adresse. . . . . : 10.23.5.55
Subnetzmaske. . . . . : 255.255.0.0
Standardgateway . . . . . : 10.23.1.254
DHCP-Server . . . . . : 10.23.3.15
DNS-Server. . . . . : 10.23.3.38
Primärer WINS-Server. . . . . : 10.23.3.16
Sekundärer WINS-Server. . . . . : 10.23.3.15
Lease erhalten. . . . . : Montag, 1. November 2004 11:29:18
Lease läuft ab. . . . . : Donnerstag, 4. November 2004 11:29:1
8
C:\>

**Abbildung C-3: MAC-Adresse/physische Adresse**

# Anhang D: Aktualisieren der Firmware

So aktualisieren Sie die Gateway-Firmware:

1. Laden Sie die Aktualisierungsdatei für die Gateway-Firmware von der Website unter *www.linksys.com/international* herunter.
2. Extrahieren Sie die Datei auf dem Computer.
3. Öffnen Sie das webbasierte Gateway-Dienstprogramm, und klicken Sie auf die Registerkarte **Administration** (Verwaltung).
4. Klicken Sie auf die Registerkarte **Firmware Upgrade** (Aktualisieren der Firmware).
5. Klicken Sie auf die Schaltfläche **Browse** (Durchsuchen), um nach der extrahierten Datei zu suchen, und doppelklicken Sie auf diese Datei.
6. Klicken Sie auf die Schaltfläche **Upgrade** (Aktualisieren), und befolgen Sie die Anweisungen auf dem Bildschirm.

**Abbildung D-1: Aktualisieren der Firmware**

# Anhang E: Glossar

**802.11b**: Ein Standard für den Wireless-Netzwerkbetrieb, der eine maximale Datenübertragungsrate von 11 MBit/s sowie eine Betriebsfrequenz von 2,4 GHz festlegt.

**802.11g**: Ein Standard für den Wireless-Netzwerkbetrieb, der eine maximale Datenübertragungsrate von 54 Mbit/s und eine Betriebsfrequenz von 2,4 GHz sowie die Abwärtskompatibilität mit Geräten festlegt, die dem Standard 802.11b entsprechen.

**Access Point**: Ein Gerät, über das Computer und andere Geräte mit Wireless-Funktionalität mit einem verdrahteten Netzwerk kommunizieren können. Wird auch verwendet, um die Reichweite von Wireless-Netzwerken zu erweitern.

**Adapter**: Ein Gerät, mit dem Ihr Computer Netzwerkfunktionalität erhält.

**Ad-Hoc**: Eine Gruppe von Wireless-Geräten, die nicht über einen Access Point, sondern direkt miteinander kommunizieren (Peer-to-Peer).

**AES** (***A**dvanced **E**ncryption **S**tandard*): Eine Sicherheitsmethode, bei der die symmetrische Datenverschlüsselung mit 128 Bit verwendet wird.

**Aktualisierung**: Das Ersetzen vorhandener Software oder Firmware durch eine neuere Version.

**Backbone**: Der Teil des Netzwerks, der die meisten Systeme und Netzwerke miteinander verbindet und die meisten Daten verarbeitet.

**Bandbreite**: Die Übertragungskapazität eines bestimmten Geräts oder Netzwerks.

**Bandspreizung**: Weitband-Funkfrequenzmethode, die für eine zuverlässigere und sicherere Datenübertragung verwendet wird.

**Beacon-Intervall**: Im Wireless-Netzwerk übertragene Daten zur Synchronisierung des Netzwerks.

**Bit**: Eine binäre Informationseinheit.

**Bridge**: Ein Gerät, das verschiedene Netzwerke miteinander verbindet.

**Breitband**: Eine stets aktive, schnelle Internetverbindung.

**Browser**: Eine Anwendung, mit der auf alle im World Wide Web enthaltenen Informationen interaktiv zugegriffen werden kann.

**Byte**: Eine Dateneinheit, die üblicherweise aus acht Bit besteht.

**CSMA/CA** (***C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **A**voidance*): Eine Datenübertragungsmethode, die verwendet wird, um Datenkollisionen zu verhindern.

**CTS** (***C**lear **T**o **S**end*): Ein von einem Wireless-Gerät gesendetes Signal, das angibt, dass das Gerät für Daten empfangsbereit ist.

**Daisy Chain** (Verkettung): Eine Methode, bei der Geräte in Reihe (in einer Kette) miteinander verbunden werden.

**Datenbank**: Eine Datensammlung, die so organisiert ist, dass die enthaltenen Daten schnell und einfach verwaltet und aktualisiert werden können sowie problemlos abrufbar sind.

**DDNS** (***D**ynamic **D**omain **N**ame **S**ystem*): Ein System, in dem eine Website, ein FTP- oder E-Mail-Server mit einem festen Domänennamen (z. B. www.xyz.com) eine dynamische IP-Adresse verwenden kann.

**DHCP** (***D**ynamic **H**ost **C**onfiguration **P**rotocol*): Ein Netzwerkprotokoll, mit dem Administratoren Netzwerkcomputern temporäre IP-Adressen zuweisen können, indem sie IP-Adressen für einen bestimmten Zeitraum an Benutzer „vermieten“ statt ihnen eine permanente IP-Adresse zuzuweisen.

**DMZ** (***Dem**ilitarized **Z**one*): Hebt den Firewall-Schutz des Routers für einen PC auf, sodass dieser im Internet „sichtbar“ wird.

**DNS** (***D**omain **N**ame **S**erver*): Die IP-Adresse des Servers Ihres Internetdienstanbieters, der die Namen von Websites in IP-Adressen übersetzt.

**Domäne**: Ein spezifischer Name für ein Netzwerk aus mehreren Computern.

**DSL** (***D**igital **S**ubscriber **L**ine*): Eine stets aktive Breitbandverbindung über herkömmliche Telefonleitungen.

**DSSS** (***D**irect-**S**equence **S**pread-**S**pectrum*): Eine Frequenzübertragungstechnologie, die ein redundantes Bit-Muster verwendet, um die Wahrscheinlichkeit von Datenverlusten bei der Übertragung zu senken.

**DTIM** (***D**elivery **T**raffic **I**ndication **M**essage*): Eine in Datenpaketen enthaltene Nachricht, die zur Verbesserung der Effizienz von Wireless-Verbindungen beitragen kann.

**Durchsatz**: Die Datenmenge, die in einem bestimmten Zeitraum erfolgreich von einem Knoten an einen anderen übertragen werden kann.

**Dynamische IP-Adresse**: Eine von einem DHCP-Server zugewiesene temporäre IP-Adresse.

**EAP** (***E**xtensible **A**uthentication **P**rotocol*): Ein allgemeines Authentifizierungsprotokoll zur Steuerung des Netzwerkzugriffs. Viele spezielle Authentifizierungsmethoden greifen auf dieses Protokoll zurück.

**EAP-PEAP** (***E**xtensible **A**uthentication **P**rotocol-**P**rotected **E**xtensible **A**uthentication **P**rotocol*): Eine gegenseitige Authentifizierungsmethode, bei der eine Kombination von digitalen Zertifikaten sowie ein anderes System, z. B. Passwörter, verwendet werden.

**EAP-TLS** (***E**xtensible **A**uthentication **P**rotocol-**T**ransport **L**ayer **S**ecurity*): Eine gegenseitige Authentifizierungsmethode, bei der digitale Zertifikate verwendet werden.

**Ethernet**: Ein Netzwerkprotokoll, mit dem festgelegt wird, wie Daten auf gängigen Übertragungsmedien gespeichert und von dort abgerufen werden.

**Finger**: Ein Programm, das Ihnen den Namen angibt, der einer E-Mail-Adresse zugewiesen ist.

**Firewall**: Eine Gruppe von Programmen, die sich auf einem Netzwerk-Gateway-Server befindet und die Ressourcen des Netzwerks vor unberechtigten Benutzern schützt.

**Firmware**: Der für den Betrieb eines Netzwerkgeräts verwendete Programmcode.

**Fragmentierung**: Das Aufteilen von Paketen in kleinere Einheiten bei der Übertragung über Netzwerkmedien, die die ursprüngliche Größe des Pakets nicht unterstützen.

**FTP** (***F**ile **T**ransfer **P**rotocol*): Ein Protokoll für die Übertragung von Dateien über ein TCP/IP-Netzwerk.

**Gateway**: Ein Gerät zur Verbindung von Netzwerken mit unterschiedlichen, inkompatiblen Kommunikationsprotokollen.

**Halbduplex**: Datenübertragung, die über eine Leitung in beide Richtungen erfolgt, jedoch entweder in die eine oder die andere Richtung, nicht gleichzeitig in beide.

**Hardware**: Als Hardware bezeichnet man die physischen Geräte im Computer- und Telekommunikationsbereich sowie andere Informationstechnologiegeräte.

**Herunterladen**: Das Empfangen einer Datei, die über ein Netzwerk übertragen wurde.

**Hochfahren**: Starten von Geräten, sodass diese Befehle ausführen.

**HTTP** (***H**yper**T**ext **T**ransport **P**rotocol*): Kommunikationsprotokoll, mit dem Verbindungen zu Servern im World Wide Web hergestellt werden.

**Infrastruktur**: Ein Wireless-Netzwerk, das über einen Access Point mit einem verdrahteten Netzwerk verbunden ist.

**IP** (***I**nternet **P**rotocol*): Ein Protokoll zum Senden von Daten über Netzwerke.

**IP-Adresse**: Die Adresse, anhand der ein Computer oder ein Gerät im Netzwerk identifiziert werden kann.

**IPCONFIG**: Ein Dienstprogramm für Windows 2000 und Windows XP, das die IP-Adresse für ein bestimmtes Netzwerkgerät anzeigt.

**IPSec** (***I**nternet **P**rotocol **Sec**urity*): Ein VPN-Protokoll, das für den sicheren Austausch von Paketen auf der IP-Ebene verwendet wird.

**ISM-Band**: Bei Übertragungen im Wireless-Netzwerkbetrieb verwendete Funkbandbreite.

**ISP** (***I**nternet **S**ervice **P**rovider*): Internetdienstanbieter; ein Anbieter, über den auf das Internet zugegriffen werden kann.

**Kabelmodem**: Ein Gerät, über das ein Computer mit dem Kabelfernsehnetzwerk verbunden wird, das wiederum eine Verbindung zum Internet herstellt.

**Knoten**: Ein Netzwerkknotenpunkt bzw. -verbindungspunkt, üblicherweise ein Computer oder eine Arbeitsstation.

**Laden**: Das Übertragen einer Datei über das Netzwerk.

**LAN**: Die Computer und Netzwerkprodukte, aus denen sich Ihr lokales Netzwerk zusammensetzt.

**LEAP** (***L**ightweight **E**xtensible **A**uthentication **P**rotocol*): Eine gegenseitige Authentifizierungsmethode, bei der ein Benutzername- und Passwortsystem verwendet wird.

**MAC-Adresse** (***M**edia **A**ccess **C**ontrol*): Die eindeutige Adresse, die ein Hersteller jedem einzelnen Netzwerkgerät zuweist.

**MBit/s** (***M**ega**bit** pro **S**ekunde*): Eine Million Bit pro Sekunde. Maßeinheit für die Datenübertragung.

**mIRC**: Ein unter Windows verwendetes Internet Relay Chat-Programm.

**Multicasting**: Das gleichzeitige Senden von Daten an mehrere Ziele.

**NAT** (***N**etwork **A**ddress **T**ranslation*): Die NAT-Technologie übersetzt IP-Adressen von lokalen Netzwerken in eine andere IP-Adresse für das Internet.

**Netzwerk**: Mehrere Computer oder Geräte, die miteinander verbunden sind, damit Benutzer Daten gemeinsam verwenden, speichern und untereinander übertragen können.

**NNTP** (***N**etwork **N**ews **T**ransfer **P**rotocol*): Das Protokoll, mit dem eine Verbindung zu Usenet-Gruppen im Internet hergestellt wird.

**OFDM** (***O**rthogonal **F**requency **D**ivision **M**ultiplexing*): Eine Frequenzübertragungstechnologie, die den Datenstrom in mehrere Datenströme von geringerer Geschwindigkeit aufteilt, die dann parallel übertragen werden, um zu verhindern, dass Informationen während der Übertragung verloren gehen.

**Paket**: Eine Dateneinheit, die über Netzwerke gesendet wird.

**Passphrase**: Wird wie ein Passwort verwendet und erleichtert die WEP-Verschlüsselung, indem für Linksys Produkte automatisch WEP-Verschlüsselungsschlüssel erstellt werden.

**PEAP** (***P**rotected **E**xtensible **A**uthentication **P**rotocol*): Eine gegenseitige Authentifzierungsmethode, bei der eine Kombination aus digitalen Zertifikaten und einem anderen System, z. B. Passwörter, verwendet wird.

**Ping** (***P**acket **IN**ternet **G**roper*): Ein Internetdienstprogramm, mit dem ermittelt werden kann, ob eine bestimmte IP-Adresse online ist.

**PoE** (***P**ower **o**ver **E**thernet*): Eine Technologie, mit der über Ethernet-Netzwerkkabel sowohl Daten als auch Strom übertragen werden kann.

**POP3** (***P**ost **O**ffice **P**rotocol **3***): Ein im Internet verbreitet eingesetzter Standard-Mail-Server.

**Port**: Der Anschlusspunkt an einem Computer oder Netzwerkbetriebsgerät, an den Kabel oder Adapter angeschlossen werden.

**PPPoE** (***P**oint to **P**oint **P**rotocol **o**ver **E**thernet*): Eine Art der Breitbandverbindung, die neben der Datenübertragung eine Authentifizierungsmöglichkeit (Benutzername und Passwort) bietet.

**PPTP** (***P**oint-to-**P**oint **T**unneling **P**rotocol*): Ein VPN-Protokoll, mit dem das Point-to-Point-Protokoll (PPP) über einen Tunnel durch das IP-Netzwerk geleitet werden kann. Dieses Protokoll wird darüber hinaus in Europa als eine Art der Breitbandverbindung verwendet.

**Präambel**: Teil des Wireless-Signals, mit dem der Netzwerkdatenverkehr synchronisiert wird.

**Puffer**: Puffer sind freigegebene oder zugewiesene Speicherbereiche zur Unterstützung und Koordinierung von verschiedenen Computer- und Netzwerkaktivitäten, damit sich diese nicht gegenseitig behindern oder aufhalten.

**RADIUS** (***R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice*): Ein Protokoll zur Überwachung des Netzwerkzugriffs mithilfe eines Authentifizierungsservers.

**RJ-45** (***R**egistered **J**ack-**45***): Ethernet-Anschluss für bis zu acht Drähte.

**Roaming**: Die Möglichkeit, mit einem Wireless-Gerät aus einem Access Point-Bereich in einen anderen zu wechseln, ohne dass die Verbindung unterbrochen wird.

**Router**: Ein Netzwerkgerät, mit dem mehrere Netzwerke miteinander verbunden werden.

**RTS** (***R**equest **T**o **S**end*): Eine Methode zur Koordination von großen Datenpaketen in einem Netzwerk mithilfe der RTS-Schwelle.

**Server**: Ein beliebiger Computer, der innerhalb eines Netzwerks dafür sorgt, dass Benutzer auf Dateien zugreifen, kommunizieren sowie Druckvorgänge und andere Aktionen ausführen können.

**SMTP** (***S**imple **M**ail **T**ransfer **P**rotocol*): Das standardmäßige E-Mail-Protokoll im Internet.

**SNMP** (***S**imple **N**etwork **M**anagement **P**rotocol*): Ein weit verbreitetes und häufig verwendetes Protokoll zur Netzwerküberwachung und -steuerung.

**Software**: Befehle für den Computer. Ein Satz an Befehlen, mit denen eine bestimmte Aufgabe ausgeführt wird, bezeichnet man als „Programm“.

**SOHO** (***S**mall **O**ffice/**H**ome **O**ffice*): Marktsegment der Geschäftkunden, die zu Hause oder in kleineren Büros arbeiten.

**SPI-Firewall** (***S**tateful **P**acket **I**nspection*): Eine Technologie, mit der eingehende Datenpakete vor der Weiterleitung an das Netzwerk überprüft werden.

**SSID** (***S**ervice **S**et **ID**entifier*): Der Name Ihres Wireless-Netzwerks.

**Standard-Gateway**: Ein Gerät, über das der Internetdatenverkehr Ihres LANs weitergeleitet wird.

**Statische IP-Adresse**: Eine feste Adresse, die einem in ein Netzwerk eingebundenen Computer oder Gerät zugewiesen ist.

**Statisches Routing**: Das Weiterleiten von Daten in einem Netzwerk über einen festen Pfad.

**Subnetzmaske**: Ein Adressencode, der die Größe des Netzwerks festlegt.

**Switch**: 1. Ein Daten-Switch, der Rechner mit Host-Computern verbindet, wodurch eine begrenzte Anzahl von Ports von mehreren Geräten gemeinsam genutzt werden kann. 2. Ein Gerät zum Herstellen, Trennen und Ändern der Verbindungen innerhalb von elektrischen Schaltkreisen (Schalter).

**TCP** (***T**ransmission **C**ontrol **P**rotocol*): Ein Netzwerkprotokoll zur Datenübertragung, bei dem eine Bestätigung des Empfängers der gesendeten Daten erforderlich ist.

**TCP/IP** (***T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol*): Ein Satz von Anweisungen, den alle PCs für die Kommunikation über Netzwerke verwenden.

**Telnet**: Benutzerbefehl und TCP/IP-Protokoll zum Zugriff auf Remote-PCs.

**TFTP** (***T**rivial **F**ile **T**ransfer **P**rotocol*): Eine Version des TCP/IP-FTP-Protokolls, das über keinerlei Verzeichnis- oder Passwortfunktionalitäten verfügt.

**TKIP** (***T**emporal **K**ey **I**ntegrity **P**rotocol*): Eine Wireless-Verschlüsselungsmethode, bei der für jedes übertragene Datenpaket dynamische Verschlüsselungsschlüssel zur Verfügung stehen.

**Topologie**: Die physische Anordnung eines Netzwerks.

**TX-Rate**: Übertragungsrate.

**UDP** (***U**ser **D**atagram **P**rotocol*): Ein Netzwerkprotokoll zur Datenübertragung, bei dem keine Bestätigung vom Empfänger der gesendeten Daten erforderlich ist.

**URL** (***U**niform **R**esource **L**ocator*): Die Adresse einer im Internet befindlichen Datei.

**Verschlüsselung**: Die Codierung von Daten, die über Netzwerke übertragen werden.

**Vollduplex**: Die Fähigkeit eines Netzwerkgeräts, Daten gleichzeitig empfangen und übertragen zu können.

**VPN** (***V**irtual **P**rivate **N**etwork*): Eine Sicherheitsmaßnahme, mit der Daten geschützt werden, wenn sie über das Internet von einem Netzwerk in ein anderes übertragen werden.

**WAN** (***W**ide **A**rea **N**etwork*): Das Internet.

**WEP** (**W***ired **E**quivalent **P**rivacy*): Eine hochgradig sichere Methode zum Verschlüsseln von Netzwerkdaten, die in Wireless-Netzwerken übertragen werden.

**WINIPCFG**: Ein Dienstprogramm für Windows 98 und Windows ME, das die IP-Adresse für ein bestimmtes Netzwerkgerät anzeigt.

**WLAN** (***W**ireless **L**ocal **A**rea **N**etwork*): Mehrere Computer und Geräte, die über Wireless-Verbindungen miteinander kommunizieren.

**WPA** (***W**i-Fi **P**rotected **A**ccess*): Ein Wireless-Sicherheitsprotokoll, bei dem eine TKIP-Verschlüsselung (*Temporal Key Integrity Protocol*) verwendet wird, die zusammen mit einem RADIUS-Server eingesetzt werden kann.

# Anhang F: Spezifikationen

| | |
|---|---|
| Modellnummer | WAG54GX2 |
| Standards | IEEE 802.11g, IEEE 802.11b, IEEE 802.3u, IEEE 802.3, g.992.1 (g.dmt), g.992.2 (g.lite), g.992.3, g.992.5, T1.413i2, UR-2 Deutsche Telekom |
| Ports | Power (Netzstrom), ADSL, Ethernet (1-4) |
| Tasten | Reset, Ein/Aus-Schalter |
| Kabeltyp | Kat. 5 UTP |
| LEDs | Power (Netzstrom), Wireless, Ethernet (1-4), DSL, Internet |
| Anzahl der Antennen | 2 |
| Antennenanschluss-Typ | Fest (nicht abnehmbar) |
| RF-Leistung (EIRP) in dBm | 802.11b: 18, 802.11g: 16, 820.11g MIMO: 17 |
| Antennengewinn in dBi | 3,3 |
| UPnP-fähig/ -zertifiziert | UPnP-fähig |

| | |
|---|---|
| Sicherheitsmerkmale | Passwortgeschützte Konfiguration für Web-Zugriff<br>PAP- und CHAP-Authentifizierung<br>DoS-Schutz (*Denial of Service*)<br>URL-Filterung sowie Blockieren von Stichwörtern, Java, ActiveX, Proxy und Cookies<br>ToD-Filter (Blockieren des Zugriffs nach Zeit)<br>VPN-Passthrough für IPSec-, PPTP- und L2TP-Protokolle<br>WEP (128/64 Bit) mit Passphrasen-/WEP-Schlüsselerstellung<br>Deaktivierung der SSID-Übertragung<br>Zugriffsbeschränkung nach MAC- und IP-Adressen<br>Unterstützung von bis zu 5 IPsec VPN-Terminal-Tunneln<br>Unterstützung für WPA und WPA2 |
| WEP-Schlüssel | 64 Bit, 128 Bit |
| Abmessungen | 140 mm x 140 mm x 27 mm |
| Gewicht | 0,27 kg |
| Stromversorgung | 12 V=, 1 A |
| Zertifizierungen | CE |
| Betriebstemperatur | 0 ºC bis 40 ºC |
| Lagertemperatur | -20 ºC bis 70 ºC |
| Betriebsfeuchtigkeit | 10 % bis 85 %, nicht kondensierend |
| Lagerfeuchtigkeit | 5 % bis 90 %, nicht kondensierend |

# Anhang G: Garantieinformationen

Linksys sichert Ihnen für einen Zeitraum von drei Jahren (die „Gewährleistungsfrist“) zu, dass dieses Linksys Produkt bei normaler Verwendung keine Material- oder Verarbeitungsfehler aufweist. Im Rahmen dieser Gewährleistung beschränken sich Ihre Rechtsmittel und der Haftungsumfang von Linksys wie folgt: Linksys kann nach eigener Wahl das Produkt reparieren oder austauschen oder Ihnen den Kaufpreis abzüglich etwaiger Nachlässe zurückerstatten. Diese eingeschränkte Gewährleistung gilt nur für den ursprünglichen Käufer.

Sollte sich das Produkt während der Gewährleistungsfrist als fehlerhaft erweisen, wenden Sie sich an den technischen Support von Linksys, um eine so genannte *Return Authorization Number* (Nummer zur berechtigten Rücksendung) zu erhalten. WENN SIE SICH AN DEN TECHNISCHEN SUPPORT WENDEN, SOLLTEN SIE IHREN KAUFBELEG ZUR HAND HABEN. Wenn Sie gebeten werden, das Produkt einzuschicken, geben Sie die Nummer zur berechtigten Rücksendung gut sichtbar auf der Verpackung an, und legen Sie eine Kopie des Originalkaufbelegs bei. RÜCKSENDEANFRAGEN KÖNNEN NICHT OHNE DEN KAUFBELEG BEARBEITET WERDEN. Der Versand fehlerhafter Produkte an Linksys erfolgt auf Ihre Verantwortung. Linksys kommt nur für Versandkosten von Linksys zu Ihrem Standort per UPS auf dem Landweg auf. Bei Kunden außerhalb der USA und Kanadas sind sämtliche Versand- und Abfertigungskosten durch die Kunden selbst zu tragen.

ALLE GEWÄHRLEISTUNGEN UND BEDINGUNGEN STILLSCHWEIGENDER ART HINSICHTLICH DER MARKTÜBLICHEN QUALITÄT ODER DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK SIND AUF DIE DAUER DER GEWÄHRLEISTUNGSFRIST BESCHRÄNKT. JEGLICHE WEITEREN BEDINGUNGEN, ZUSICHERUNGEN UND GEWÄHRLEISTUNGEN SOWOHL AUSDRÜCKLICHER ALS AUCH STILLSCHWEIGENDER ART, EINSCHLIESSLICH JEGLICHER STILLSCHWEIGENDER GEWÄHRLEISTUNG DER NICHTVERLETZUNG, WERDEN AUSGESCHLOSSEN. Einige Gerichtsbarkeiten gestatten keine Beschränkungen hinsichtlich der Gültigkeitsdauer einer stillschweigenden Gewährleistung; die oben genannte Beschränkung findet daher unter Umständen auf Sie keine Anwendung. Die vorliegende Gewährleistung sichert Ihnen bestimmte gesetzlich verankerte Rechte zu. Darüber hinaus stehen Ihnen je nach Gerichtsbarkeit unter Umständen weitere Rechte zu.

Diese Gewährleistung gilt nicht, wenn das Produkt (a) von einer anderen Partei als Linksys verändert wurde, (b) nicht gemäß den von Linksys bereitgestellten Anweisungen installiert, betrieben, repariert oder gewartet wurde oder (c) unüblichen physischen oder elektrischen Belastungen, Missbrauch, Nachlässigkeit oder Unfällen ausgesetzt wurde. Darüber hinaus kann Linksys angesichts der ständigen Weiterentwicklung neuer Methoden zum unerlaubten Zugriff und Angriff auf Netzwerke nicht gewährleisten, dass das Produkt keinerlei Schwachstellen für unerlaubte Zugriffe oder Angriffe bietet.

SOWEIT NICHT GESETZLICH UNTERSAGT, SCHLIESST LINKSYS JEGLICHE HAFTUNG FÜR VERLOREN GEGANGENE DATEN, ENTGANGENE EINNAHMEN, ENTGANGENE GEWINNE ODER SONSTIGE SCHÄDEN BESONDERER, INDIREKTER, MITTELBARER, ZUFÄLLIGER ODER BESTRAFENDER ART AUS, DIE SICH AUS DER VERWENDUNG BZW. DER NICHTVERWENDBARKEIT DES PRODUKTS (AUCH DER SOFTWARE) ERGEBEN ODER MIT DIESER ZUSAMMENHÄNGEN, UNABHÄNGIG VON DER HAFTUNGS-THEORIE (EINSCHLIESSLICH NACHLÄSSIGKEIT), AUCH WENN LINKSYS ÜBER DIE MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE. DIE HAFTUNG VON LINKSYS IST STETS AUF DEN FÜR DAS PRODUKT GEZAHLTEN BETRAG BESCHRÄNKT. Die oben genannten Beschränkungen kommen auch dann zur Anwendung, wenn eine in diesem Abschnitt aufgeführte Gewährleistung oder Zusicherung ihren wesentlichen Zweck verfehlt. Einige Gerichtsbarkeiten gestatten keinen Ausschluss von bzw. keine Beschränkungen auf zufällige oder Folgeschäden; die oben genannte Beschränkung oder der oben genannte Ausschluss findet daher unter Umständen auf Sie keine Anwendung.

**Die vorliegende Gewährleistung ist nur in dem Land gültig bzw. kann nur in dem Land verarbeitet werden, in dem das Produkt erworben wurde.**

Richten Sie alle Anfragen direkt an: Linksys, P.O. Box 18558, Irvine, CA 92623, USA

# Anhang H: Zulassungsinformationen

FCC-Bestimmungen

Dieses Gerät wurde geprüft und entspricht den Bestimmungen für ein digitales Gerät der Klasse B gemäß Teil 15 der FCC-Bestimmungen. Die Grenzwerte wurden so festgelegt, dass ein angemessener Schutz gegen Störungen in einer Wohngegend gewährleistet ist. Dieses Gerät erzeugt und verwendet Hochfrequenzenergie und kann diese abstrahlen. Wird es nicht gemäß den Angaben des Herstellers installiert und betrieben, kann es sich störend auf den Rundfunk- und Fernsehempfang auswirken. Es besteht jedoch keine Gewähr, dass bei einer bestimmten Installation keine Störungen auftreten. Sollte dieses Gerät Störungen des Radio- und Fernsehempfangs verursachen (was durch Ein- und Ausschalten des Geräts feststellbar ist), wird der Benutzer aufgefordert, die Störungen durch eine oder mehrere der folgenden Maßnahmen zu beheben:

- Richten Sie die Empfangsantenne neu aus, oder stellen Sie sie an einem anderen Ort auf.
- Increase the separation between the equipment or devices.
- Schließen Sie das Gerät an eine anderen Anschluss als den des Empfängers an.
- Wenden Sie sich bei Fragen an Ihren Händler oder an einen erfahrenen Funk-/Fernsehtechniker.

FCC-Bestimmungen zur Freisetzung gefährlicher Strahlung

Dieses Gerät erfüllt die FCC-Bestimmungen zur Freisetzung gefährlicher Strahlung in einer nicht gesteuerten Umgebung. Dieses Gerät sollte so installiert und betrieben werden, dass der Abstand zwischen dem Radiator und Personen mindestens 20 cm beträgt.

INDUSTRY CANADA (CANADA)

Dieses Gerät erfüllt die kanadischen Bestimmungen der Richtlinien ICES-003 und RSS210.

Cet appareil est conforme aux normes NMB-003 et RSS210 d'Industry Canada.

## Informationen zur Einhaltung gesetzlicher Vorschriften bei 2,4-GHz-Wireless-Produkten für den Bereich der EU und anderer Länder gemäß EU-Richtlinie 1999/5/EG (R&TTE-Richtlinie)

### Konformitätserklärung zur EU-Richtlinie 1999/5/EG (R&TTE-Richtlinie)

| | |
|---|---|
| Česky [Czech]: | Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC. |
| Dansk [Danish]: | Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF. |
| Deutsch [German]: | Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU. |
| Eesti [Estonian]: | See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele. |
| English: | This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. |
| Español [Spanish]: | Este equipo cumple con los requisitos esenciales asi como con otras disposiciones de la Directiva 1999/5/CE. |
| Ελληνική [Greek]: | Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC. |
| Français [French]: | Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC. |
| Íslenska [Icelandic]: | Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC. |
| Italiano [Italian]: | Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE. |
| Latviski [Latvian]: | Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. |
| Lietuvių [Lithuanian]: | Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas. |
| Nederlands [Dutch]: | Dit apparaat voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC. |
| Malti [Maltese]: | Dan l-apparat huwa konformi mal-ħtiġiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC. |
| Margyar [Hungarian]: | Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket. |

| | |
|---|---|
| Norsk [Norwegian]: | Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF. |
| Polski [Polish]: | Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/EC. |
| Português [Portuguese]: | Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC. |
| Slovensko [Slovenian]: | Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/EC. |
| Slovensky [Slovak]: | Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 1999/5/EC. |
| Suomi [Finnish]: | Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen. |
| Svenska [Swedish]: | Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC. |

**HINWEIS:** Für alle Produkte ist die Konformitätserklärung in folgender Form verfügbar:

- PDF-Datei auf der Produkt-CD.
- Druckversion im Lieferumfang des Produkts.
- PDF-Datei auf der Produkt-Webseite. Rufen Sie www.linksys.com/international auf, und wählen Sie das für Sie zutreffende Land bzw. die entsprechende Region aus. Wählen Sie dann Ihr Produkt aus.

Wenn Sie weitere technische Dokumente benötigen, finden Sie entsprechende Hinweise im Abschnitt „Technische Dokumente unter www.linksys.com/international“ weiter hinten in diesem Anhang.

Bei der Bewertung des Produkts hinsichtlich der Anforderungen der Richtlinie 1999/5/EG kamen die folgenden Standards zur Anwendung:

- Funkausrüstung: EN 300 328
- EMV: EN 301 489-1, EN 301 489-17
- Sicherheit: EN 60950

CE-Kennzeichnung

Die Wireless-B- und Wireless-G-Produkte von Linksys sind mit der folgenden CE-Kennzeichnung, der Nummer der Überwachungs- und Zertifizierungsstelle (sofern zutreffend) und der Kennung der Klasse 2 versehen.

CE 0560 ! oder CE 0678 ! oder CE !

Überprüfen Sie das CE-Etikett auf dem Produkt, um die Überwachungs- und Zertifizierungsstelle zu ermitteln, die in die Bewertung einbezogen wurde.

Nationale Beschränkungen

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

*Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:*

*Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesii menzionati di seguito:*

*Das Produkt kann in allen EU-Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten, die der EU-Richtlinie 1999/5/EG folgen), mit Ausnahme der folgenden Staaten:*

Belgien

Wireless-Verbindungen im Freien mit einer Reichweite über 300 m müssen beim Belgischen Institut für Postdienste und Telekommunikation (BIPT) angemeldet werden. Weitere Informationen finden Sie unter http://www.bipt.be.

*Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.*

*Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.*

Frankreich

Bei Verwendung des Produkts im Freien gelten für die Ausgangsleistung in bestimmten Bandbereichen Beschränkungen. Weitere Informationen finden Sie in Tabelle 1 oder unter http://www.art-telecom.fr/.

*Dans le cas d'une utilisation en extérieur, la puissance de sortie est limitée pour certaines parties de la bande. Reportez-vous à la table 1 ou visitez http://www.art-telecom.fr/ pour de plus amples détails.*

Tabelle 1: In Frankreich zulässige Leistungspegel

| **Standort** | **Frequenzbereich (MHz)** | **Leistung (EIRP; *Effective Isotropic Radiated Power*)** |
|---|---|---|
| In Gebäuden (keine Beschränkungen) | 2400-2483,5 | 100 mW (20 dBm) |
| Im Freien | 2400-2454<br>2454-2483,5 | 100 mW (20 dBm)<br>10 mW (10 dBm) |

Italien

Dieses Produkt entspricht den nationalen Vorschriften für Funkschnittstellen und den in der nationalen Frequenzzuweisungstabelle für Italien aufgeführten Anforderungen. Für den Betrieb dieses 2,4-GHz-Wireless-LAN-Produkts außerhalb der Grundstücksgrenzen des Eigentümers ist eine allgemeine Genehmigung erforderlich. Weitere Informationen finden Sie unter http://www.comunicazioni.it/it/.

*Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN a 2.4 GHz richiede una "Autorizzazione Generale". Consultare http://www.comunicazioni.it/it/ per maggiori dettagli.*

Beschränkungen hinsichtlich der Verwendung des Produkts

Dieses Produkt wurde ausschließlich für die Verwendung in Gebäuden entwickelt. Die Verwendung im Freien wird nicht empfohlen.

Dieses Produkt wurde für die Verwendung mit der im Lieferumfang enthaltenen standardmäßigen, integrierten bzw. externen (speziell für diesen Zweck vorgesehenen) Antenne entwickelt. Manche Anwendungen setzen jedoch unter Umständen voraus, dass Sie die Antenne(n) vom Produkt trennen (sofern diese abnehmbar sind) und mithilfe eines Verlängerungskabels an einem anderen Ort als das Gerät installieren. Für diese Anwendungen bietet Linksys ein R-SMA-Verlängerungskabel (AC9SMA) und ein R-TNC-Verlängerungskabel (AC9TNC). Beide Kabel sind neun Meter lang. Der Verlust durch das Kabel (die Abschwächung) liegt bei 5 dB. Zur Kompensation der Abschwächung bietet Linksys außerdem die Hochleistungsantennen HGA7S (mit R-SMA-Stecker) und HGA7T (mit R-TNC-Stecker). Diese Antennen verfügen über einen Antennengewinn von 7 dBi und dürfen nur mit dem R-SMA- oder R-TNC-Verlängerungskabel eingesetzt werden.

Kombinationen von Verlängerungskabeln und Antennen, die zu einem ausgestrahlten Leistungspegel von mehr als 100 mW EIRP (*Effective Isotropic Radiated Power*) führen, sind unzulässig.

Ausgangsleistung des Geräts

Zur Einhaltung der jeweiligen nationalen Vorschriften müssen Sie u. U. die Ausgangsleistung Ihres Wireless-Geräts anpassen. Fahren Sie mit dem entsprechenden Abschnitt für Ihr Gerät fort.

**HINWEIS:** Die Einstellungen für die Ausgangsleistung sind u. U. nicht für alle Wireless-Produkte verfügbar. Weitere Informationen finden Sie in der Dokumentation auf der Produkt-CD oder unter http://www.linksys.com/international.

Wireless-Adapter

Bei Wireless-Adaptern ist die Ausgangsleistung standardmäßig auf 100 % eingestellt. Die Ausgangsleistung der einzelnen Adapter beträgt maximal 20 dBm (100 mW), liegt aber gewöhnlich bei 18 dBm (64 mW) oder darunter. Wenn Sie die Ausgangsleistung Ihres Wireless-Adapters anpassen müssen, befolgen Sie die entsprechenden Anweisungen für das Windows-Betriebssystem Ihres Computers:

Windows XP
1. Doppelklicken Sie auf dem Desktop in der Taskleiste auf das Symbol **Drahtlose Verbindung**.
2. Öffnen Sie das Fenster *Drahtlose Netzwerkverbindung*.
3. Klicken Sie auf die Schaltfläche **Eigenschaften**.
4. Klicken Sie auf die Registerkarte **Allgemein** und dann auf die Schaltfläche **Konfigurieren**.
5. Klicken Sie im Fenster *Eigenschaften* auf die Registerkarte **Erweitert**.
6. Wählen Sie **Ausgangsleistung** aus.
7. Wählen Sie aus dem rechts angezeigten Pulldown-Menü den Prozentsatz für die Ausgangsleistung des Wireless-Adapters aus.

Windows 2000

1. Öffnen Sie das Fenster *Systemsteuerung*.
2. Doppelklicken Sie auf **Netzwerk- und DFÜ-Verbindungen**.
3. Wählen Sie Ihre aktuelle Wireless-Verbindung aus, und wählen Sie dann **Eigenschaften**.
4. Klicken Sie im Fenster *Eigenschaften* auf die Schaltfläche **Konfigurieren**.
5. Klicken Sie auf die Registerkarte **Erweitert**, und wählen Sie **Ausgangsleistung** aus.
6. Wählen Sie aus dem rechts angezeigten Pulldown-Menü die Leistungseinstellung für den Wireless-Adapter aus.

Wenn auf Ihrem Computer Windows ME oder Windows 98 ausgeführt wird, finden Sie in der Windows-Hilfe Anweisungen zum Aufrufen der erweiterten Einstellungen von Netzwerkadaptern.

Wireless Access Points, Router und andere Wireless-Produkte

Wenn Sie über einen Wireless Access Point, einen Router oder ein anderes Wireless-Produkt verfügen, verwenden Sie das zugehörige webbasierte Dienstprogramm, um die Einstellungen für die Ausgangsleistung zu konfigurieren (weitere Informationen finden Sie in der Dokumentation zum jeweiligen Produkt).

## Technische Dokumente unter www.linksys.com/international

Führen Sie die folgenden Schritte aus, um auf die gewünschten technischen Dokumente zuzugreifen:

1. Navigieren Sie mit dem Browser zur Website http://www.linksys.com/international.
2. Klicken Sie auf Ihre Region.
3. Klicken Sie auf den Namen Ihres Landes.
4. Klicken Sie auf **Produkt**.
5. Klicken Sie auf die entsprechende Produktkategorie.
6. Wählen Sie ein Produkt aus.
7. Klicken Sie auf den gewünschten Dokumentationstyp. Das Dokument wird automatisch im PDF-Format geöffnet.

**HINWEIS:** Wenn Sie Fragen zur Einhaltung gesetzlicher Vorschriften in Bezug auf diese Produkte haben oder die gewünschten Informationen nicht finden können, wenden Sie sich an die Vertriebsniederlassung vor Ort. Weitere Informationen finden Sie unter http://www.linksys.com/international.

# Anhang I: Kontaktinformationen

Möchten Sie sich persönlich an Linksys wenden?
Informationen zu den aktuellen Produkten und Aktualisierungen für bereits installierte Produkte finden Sie online unter:
http://www.linksys.com/international

Wenn Sie im Zusammenhang mit Linksys Produkten auf Probleme stoßen, können Sie uns unter folgenden Adressen eine E-Mail senden:

| In Europa | E-Mail-Adresse |
|---|---|
| Belgien | support.be@linksys.com |
| Dänemark | support.dk@linksys.com |
| Deutschland | support.de@linksys.com |
| Frankreich | support.fr@linksys.com |
| Großbritannien & Irland | support.uk@linksys.com |
| Italien | support.it@linksys.com |
| Niederlande | support.nl@linksys.com |
| Norwegen | support.no@linksys.com |
| Österreich | support.at@linksys.com |
| Portugal | support.pt@linksys.com |
| Schweden | support.se@linksys.com |
| Schweiz | support.ch@linksys.com |
| Spanien | support.es@linksys.com |

| Außerhalb von Europa | E-Mail-Adresse |
|---|---|
| Asien-Pazifik | asiasupport@linksys.com (nur Englisch) |
| Lateinamerika | support.portuguese@linksys.com oder support.spanish@linksys.com |
| Naher Osten und Afrika | support.mea@linksys.com (nur Englisch) |
| USA und Kanada | support@linksys.com |